System Release 2.2.1
ASTRO ® 25
INTEGRATED VOICE AND DATA

Mobile VPN Gateway

JANUARY 2017

MN003335A01-B

Copyrights

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

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 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, 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 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 center for information about the waste collection system in their country.

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

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

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

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

North America Parts Organization

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

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

Comments

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

Provide the following information when reporting a documentation error:

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

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

This page intentionally left blank.

Document History

Version	Description	Date
MN003166A01-A	Original release of the *Mobile VPN Gateway* supporting ASTRO 25 starting at system release 7.17 and Public Safety LTE starting at system release 11.0.	November 2016
MN003166A01-B	Updated procedural notes to procedure Configuring the Network Identity on page 65 steps 14 and 18 and UIS server renamed to backup and restore management feature.	January 2017

This page intentionally left blank.

Contents

List of Figures

List of Tables

This page intentionally left blank.

List of Processes

This page intentionally left blank.

List of Procedures

About Mobile VPN Gateway

The Mobile VPN Gateway manual provides a description of the Motorola Solutions Mobile VPN Gateway hardware and software platform and includes information necessary to set up this server in a secure applications network. This manual also includes information required for operation and troubleshooting, as well as reference information for setting up and using the Mobile VPN Gateway.

What Is Covered In This Manual?

This manual contains the following chapters.

- Mobile VPN Gateway Overview on page 29 provides high-level overview of the hardware and software server platform hosting the Mobile VPN Gateway server application.
- Mobile VPN Gateway Installation on page 39 provides information and procedures to set up (install and configure) the Mobile VPN Gateway Server.
- Mobile VPN Gateway Configuration on page 61 details configuration procedures relating to an ESXi-based Virtual Server in the Motorola system.
- Mobile VPN Gateway Operations on page 111 provides procedures for operation and administration and maintenance of Mobile VPN Gateway.
- Mobile Virtual Private Network Gateway Maintenance on page 125 provides procedures for maintenance of the Mobile VPN Gateway.
- Mobile VPN Gateway Server Troubleshooting on page 133 provides information about basic troubleshooting.
- Mobile VPN Gateway FRU/FRE Information on page 151 lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) for the Mobile VPN Gateway.
- Mobile VPN Gateway Server Disaster Recovery on page 167 provides disaster recovery procedures for the Mobile VPN Gateway.
- Configuring User Equipment for Motorola Solutions VPN Service on page 171 provides procedures for configuring User Equipment of the Mobile VPN service.
- Motorola Solutions Mobile VPN Client Configuration on Android Devices on page 179 provides instructions for installation and configuration of the Mobile VPN client for non-Motorola devices.
- Licensing Administration on page 70 provides information on licensing and procedures for obtaining licenses for the Mobile VPN Gateway.

Helpful Background Information

Motorola 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

Unless otherwise specified, the Motorola documents listed here are available from Motorola Online at http://businessonline.motorolasolutions.com. If you are new to Motorola Online, follow the on-screen instructions to sign up for an account.

To access Public Safety LTE infrastructure manuals, select **Resource Center** → **Product Information** → **Manuals**. Then select the appropriate Public Safety LTE release under **Private Broadband Solutions**, or the appropriate ASTRO® 25 release under **Network Infrastructure**.

The Resource Center also provides a Search function.

Table 1: Motorola Documentation

Related Information	Purpose
Standards and Guidelines for Communication Sites (6881089E50)	Provides standards and guidelines that should be followed when setting up a Motorola communications site. Also known as the R56 manual. This manual may be purchased on CD **9880384V83**, by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
ASTRO® 25 *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.
Public Safety LTE *System and Documentation Overview* manual	Provides an introduction to the overall Public Safety Long Term Evolution (PS LTE) system offering from Motorola Solutions, and describes the associated documentation.
Public Safety LTE *Applications Network* manual	Provides examples of transport configuration options for agency applications and common applications in Public Safety LTE systems. The configuration for your organization depends on options purchased and additional applications your organization has installed at the site.
Device Management Solution (OMA)	Provides description, installation, configuration, operation, and recovery information for the centralized Device Management Solution which meets Open Mobile Alliance (OMA) requirements.
LEX *Mission Critical Handheld Service Provisioning Guides*	These guides provide complete sequences for staging and provisioning a specific model of LEX mission critical handheld in the field.
Public Safety LTE *VML750 – LTE Vehicular Subscriber Modem (VSM) Configuration Guide*	Provides general instructions for configuring the VML750 Vehicular Subscriber Modem (VSM), and for installing the Status Utility on your computer.
Public Safety LTE *VML750 Vehicular Subscriber Modem (VSM) MVPN Configuration Guide*	Provides general instructions for configuring Motorola Solutions Mobile VPN service on the VML750 using the Motorola OMA-based Device Management Server.
CRYPTR 2 Broadband IP Encryption Unit (Standard Assurance with Enterprise Software Build)	Provides instructions on installing, configuring, and using the CRYPTR 2 (Broadband IP Encryption Unit) hardware and Standard Assurance with Enterprise Software.
PSLTE Application Network	Provides instructions on BlueCat configuration for MVPN.
Operations Support Platform Backup Manager Operator Guide	Provides instructions on PS-LTE BAR solution and operating procedures for the Enhanced Software Upgrade (ESU) solution that includes a backup and restore management feature that provides the OSP Backup Manager functions.

Table 2: Non-Motorola Publications and Documentation

Related Information	Description
strongSwan documentation	Detailed information about the *strongSwan* Open Source IPsec-based VPN solution can be found at http://www.strongswan.org.
HP ProLiant DL380 Gen9 Server User Guide	Detailed information about the Gen9 server can be found at http://www.hp.com/go/docs. From the **Products and Solutions** list, select **HP ProLiant Gen9 Server**, then **HP ProLiant DL380 Gen9 Server**.
HP iLO 4 User Guide	Detailed information about HP iLO 4 can be found at http://www.hp.com/go/ilo/docs.
HP Quick Deploy Rail System Installation Instructions	Ships with product.

This page intentionally left blank.

Chapter 1

Mobile VPN Gateway Overview

This chapter provides a descriptive overview of the hardware and software server platform hosting the Motorola Solutions Mobile VPN Gateway server application.

1.1 Mobile VPN Gateway Description

The primary function of the Motorola Solutions Mobile VPN (MVPN) Gateway is to provide an encrypted communications path (a virtual private network path) between a subscriber unit and a secure applications network.

The MVPN Gateway solution is based on the Internet Protocol Security (IPsec) suite. There are three authentication methods available for the MVPN Gateway:

Pre-Shared Keys (PSK)
Pre-Shared Keys (PSK) allow for creating encrypted IPsec tunnels using predefined keys.

Public Key Infrastructure (PKI)
If a Public Key Infrastructure (PKI) certificate management solution is implemented for a system feature, the MVPN Gateway verifies the identity of secure VPN clients using the certificate provisioned from a trusted Certificate Authority (CA), and whether the certificate has expired or has been revoked.

Username and password
Username and password authentication is also available through the MVPN, using EAP-RADIUS and an Active Directory server.

1.2 Mobile VPN Gateway Clients

Mobile VPN Gateway supports specific combinations of user equipment and VPN client software.

Table 3: Relation between particular Mobile VPN Gateway Clients, Profile Type and Supported Authentication Modes

VPN Clients	Profile Type	Available Authentication
ASTRO 25 APX radio subscribers	ASTRO Subscriber	Pre-shared keys
ASTRO 25 modems, such as Sierra GX450	ASTRO Site-To-Site	Pre-shared keys
LEX mission critical handhelds with CRYPTR micro cards	Remote Access	Certificate
Vehicular subscriber modems with CRYPTR micro cards, such as the VML750	Remote Access, Site-To-Site	Certificate
Encryption/decryption devices such as CRYPTR 2	Remote Access, Site-To-Site	Certificate
Android handheld devices with Motorola VPN client installed	Remote Access	Certificate

Table continued…

VPN Clients	Profile Type	Available Authentication
Standard PC equipment with Microsoft Windows installed. For information on Windows OSes supported, see Configuring User Equipment for Motorola Solutions VPN Service on page 171.	Remote Access	User-Password

1.3 Mobile VPN Gateway Positioning in the Network Architecture

Motorola Solutions Mobile VPN (MVPN) Gateway is positioned in networks between the client device and the main network to provide secure IPsec tunnels to the clients of agency (or region) application servers. Typical network installations utilize the MVPN gateway for secure connections for remote, handheld, or vehicle-based, User Equipment (devices) in the radio network.

MVPN installations are connected to the Backhaul transport in a private or public network to the core radio interface. From the Backhaul transport, the MVPN is typically located between a firewall (switch, router) and network applications servers. An MVPN installation may be positioned as the gateway for a Secure Applications Network architecture in an agency network. The Mobile VPN Gateway connects to the network applications servers and services in the agency network.

More information regarding the positioning of the MVPN Gateway in a network is given in the following documentation:

- *System and Documentation Overview*
- *PS LTE Applications Network*

1.4 Mobile VPN Gateway Platform Characteristics

The Motorola Solutions Mobile VPN (MVPN) Gateway system provides secure access between the customer internal applications networks and the external devices networks. An HP ProLiant DL380 Gen9 Server dedicated pair of servers make up the MVPN hardware platform for high availability (redundancy).

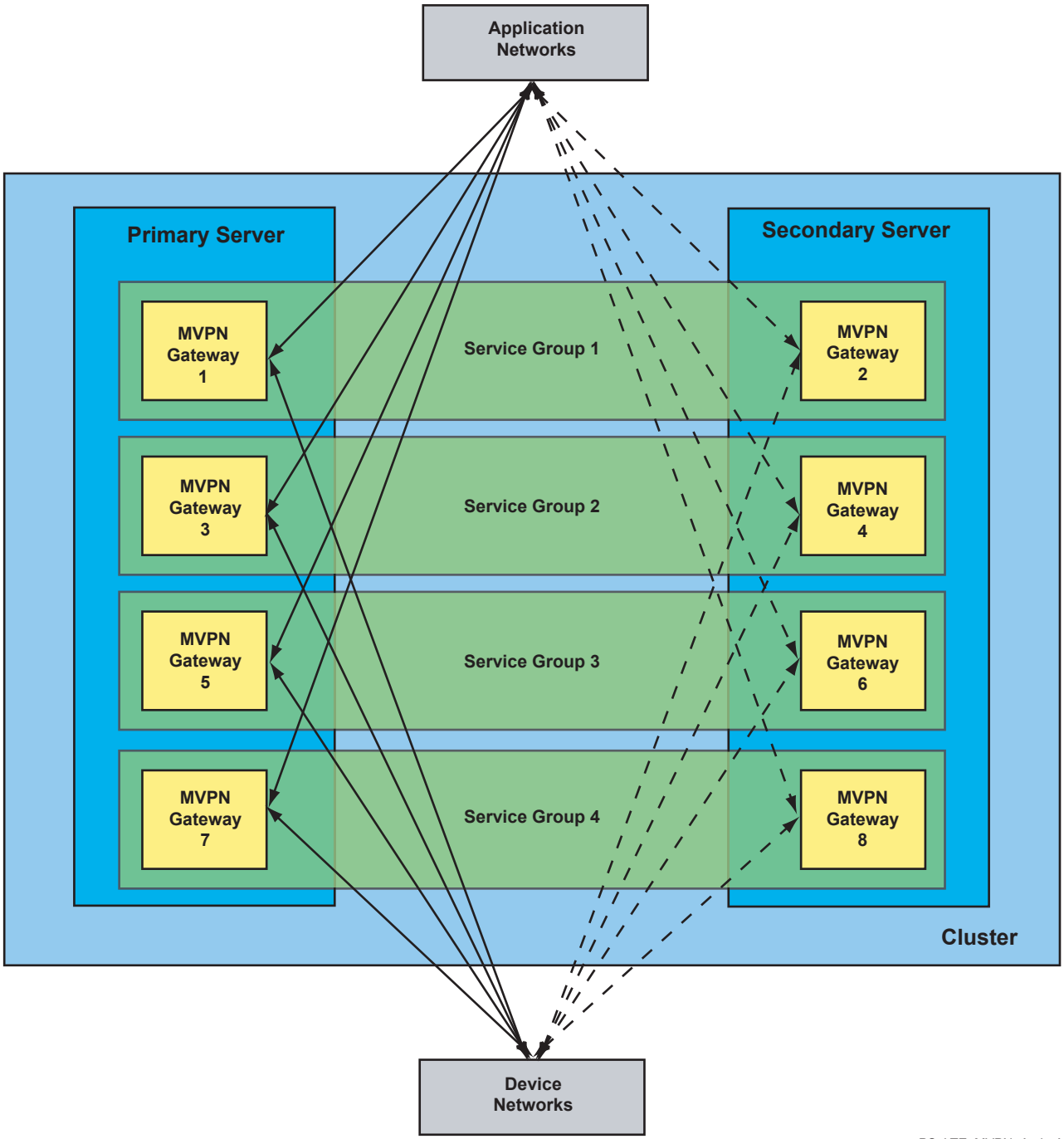
Mobile VPN (MVPN) Gateway network functionality requirements:

- The Mobile VPN Gateway requires a time source via NTP.
- Authentication with username and password requires an Active Directory server.

The primary and secondary servers are synchronized and react to outages on the primary, so that network traffic is routed to through the secondary to provide failover assurance. An in-session client connection detects a failover using a timer, and reacts to a loss of connection by re-establishing the connection to the backup MVPN virtual machine. Information, such as licensing, is automatically propagated from the primary to backup servers.

A secure communications path between the client and the network is established as needed. The client device initiates a connection to the network, and is authenticated through the MVPN. With a successful authentication, the MVPN establishes an encrypted communication path or tunnel between the client and the network.

Figure 1: MVPN Logical Architecture



The primary server contains virtual machines grouped as MVPN gateways 1, 3, 5, and 7. The secondary (redundant) server contains virtual machines grouped as MVPN gateways 2, 4, 6, and 8. These gateways and other hierarchy are shown in Figure 1: MVPN Logical Architecture on page 31.

The virtual machine gateways are further grouped as four Service Groups in the MVPN configuration. Each service group comprises a primary and secondary gateway virtual machine. All the MVPN service groups comprise the MVPN Gateway Cluster. The cluster incorporates the entire MVPN system and can be periodically backed up and restored if necessary.

1.5 Mobile VPN Gateway High Availability Option

The High Availability (HA) option is used to switch from a primary Mobile VPN Gateway server to a backup Mobile VPN Gateway Server when a failure occurs. The following types of failures are supported by the HA option:

- Loss of power
- Hardware failure
- Operating System (OS) crash or kernel panic

A redundant configuration is an active (primary) Mobile VPN Gateway and a standby (backup) Mobile VPN Gateway. These are arranged as two separate hardware/software platforms, each with a dedicated Ethernet connection (also known as HA Heartbeat) established to the network. These servers, also referred to as nodes, create a cluster with two virtual IP addresses shared between them (one per public and one per protected network).

In a redundant configuration, the allocated subsystem provides mechanisms to switch over from the active Mobile VPN Gateway to the standby Mobile VPN Gateway. When operating in a redundant configuration, the allocated subsystem provides IPsec service if one communication path fails. This eliminates the single point failure on the switch or server Ethernet port. This is achieved by (virtual) NIC teaming on the virtual servers and each cable going to a different switch. When a previously online active Mobile VPN Gateway re-joins the HA cluster, the IPsec service remains on the currently online active Mobile VPN Gateway. This prevents an unnecessary switchover.

1.6 Mobile VPN Gateway Encryption Keys and Certificate Requirements

The Motorola Solutions Mobile VPN Gateway uses the Internet Protocol Security (IPsec) protocol suite to provide secure IP packet exchange between a subscriber unit and a secure applications network, over public networks. IPsec offers cryptography-based protection services, security protocols, and dynamic key management.

A protocol within the IPsec responsible for encryption is called Encapsulating Security Payload (ESP). The IP packets, encapsulated using ESP, are sent through the IPsec virtual private network that is created in the public network.

The Mobile VPN Gateway provides three authentications methods:

- Pre-Shared Key (PSK)
- Public Key Cryptography, provided by Public Key Infrastructure (PKI)
- Username and Password (using EAP-RADIUS)

IMPORTANT: Motorola Solutions features use one method or the other. For example, Motorola Solutions Public Safety LTE application servers use only the PKI method.

For the PSK method, the parties must agree on a shared, secret key that becomes part of the IPsec policy. During the security negotiation, an authentication value derived from the pre-shared key is used to mutually authenticate the two parties during the tunnel negotiation. It is mandatory that the two parties establishing a tunnel have the exact same pre-shared key. Keys are used with algorithms (a mathematical process) to secure data. The ASTRO Subscriber and ASTRO Site-To-Site PSK keys consist of a key phrase.

Public Key Cryptography uses a pair of mathematically related cryptographic keys. A public key is freely distributed to the users, a unique private key, is kept secret. Public key is used to encrypt information, the related private key is used to decrypt that information. The person using the private key is certain that the information it is able to decrypt is intended for them. The sender of the

information can also use a digital signature to prove to a recipient that they are the source of the information. The digital signature is created using a hashing algorithm and the private key of the sender. PKI is enhanced by using digital certificates, which allow public keys to be distributed and managed.

A certificate, that is digitally signed by a Certification Authority (CA), certifies the ownership of a public key by the named subject of the certificate.

Digital certificates include:

- Information about the published identity of the owner of the corresponding private key
- Key length
- The algorithm used
- Associated hashing algorithm
- Dates of validity of the certificate
- Actions the key can be used for.

A CA is a trusted third party that is trusted by both the sender (owner of the certificate) and the recipient relying upon the certificate. Digital certificates are verified using a chain of trust. The chain of trust is an ordered list of certificates and contains an end-user subscriber certificate and intermediate certificates, that enables the receiver to verify that the sender and all intermediates certificates are trustworthy. The trust anchor for the digital certificate is the Root Certificate Authority (CA).

Agency PKI and Key Management is intended for high assurance customers who require a higher level of security and data encryption.

Authentication using EAP-RADIUS utilizes the Active Directory user accounts and credentials. To perform this type of authentication, the client sends the username/password pair to the MVPN Gateway. The MVPN Gateway does not decrypt this pair, but redirects it to the Active Directory, where it is matched against the credentials of existing VPN user accounts. If authentication was successful, the connection between the client and MVPN Gateway is established. To close the authentication loop and provide the means to authenticate not only from the client to the MVPN Gateway, but from the MVPN Gateway to the client as well, certificate chain (PKI) authentication is used.

1.7 Certificate Revocation List (CRL)

See Certificate Verification with CRL on page 138 for resolving issues related to CRL.

The imported certificate chain contains a URI (Uniform Resource Identifier) as part of the certificate. The URI is a link for the certificate revocation where the Certificate Revocation List (CRL) can be downloaded. The download of the CRL is part of the strongSwan application. The strongSwan application downloads the CRL and stores it in its local MVPN cache. By default, the time determining CRL expiration in the cache is governed by the CRL file. When client connections are established, the client certificate is compared against the downloaded version of the CRL. The client connection is denied if the client certificate is listed as revoked according to the CRL.

The new CRL is automatically downloaded at any time simply by removing the existing CRL. See Removing the Certificate Revocation List on page 92 for a procedure to remove the CRL.

The level of scrutiny for the comparison of the client certificate against the CRL can be adjusted as well. Three levels are available for the “CRL Enforcement Policy” which defines if the client certificate checked against the Certificate Revocation List (CRL) is: required, not expected or optional.

A value of “yes” means that for authentication to be successful, the following criteria is met: The certificate contains a CLR URI. This CRL URI points to the accessible location. The CRL downloaded from that CRL URI does not have the certificate in check among the list of the revoked certificates.

A value of “no” means that for authentication to be successful, the CRL downloaded from certificate CRL URI does not have the certificate in check among the list of the revoked certificates. However, it is optional for the certificate to have a CRL URI or even to have it leading to the accessible location.

A value of “ifuri” means that it is optional for certificate to have CRL URI as part of certificate. If the certificate contains the CRL URI, the authorization criteria would be established, using “yes” configuration logic. If the certificate does not contain CRL URI, the authorization criteria is established, using “no” configuration logic. See Setting Global Parameters for Connection Profiles on page 109 for a procedure to select and apply these values.

NOTICE: If the CRL Enforcement Policy is configured as “no”, and the CRL URI is present in the certificate, but points to an inaccessible location, the VPN tunnel will not be established at all as its peer cannot be verified, or its establishing or periodical key exchange takes longer than usual. (Additional time is needed for the CRL fetching timeout.)

1.8 Mobile VPN Gateway FIPS 140–2 Compliance

The MVPN Gateway is FIPS 140-2 Level 1 compliant and is using the Red Hat Enterprise Linux OpenSSL Cryptographic Module.

NOTICE: The OpenSSL Cryptographic Module is pending FIPS 140-2 Level 1 re-validation with the prior certificate #1758 as of this publication.

For end-to-end FIPS-140 compliance, the Certificate Authority (CA) issuing MVPN Gateway certificates must also be FIPS-140 compliant. Determination of the CA compliance is a customer responsibility.

1.9 GEO Redundancy

PSLTE 11 release introduces general Geo-Redundancy feature. For MVPN functionality, the following elements build up the MVPN Geo-Redundancy:

- Geo-Redundant MVPN cluster
- BLACK and RED DNS integration
- OSPF automatic routing configuration

1.9.1 Local and Geo-Redundancy Features

In addition to a local redundancy (High Availability), Mobile VPN solution offers a second redundancy model called Geo-redundancy. Mobile VPN Gateway Local and Geo redundancy modes work independently from one another and serve their own purpose.

In local redundancy mode, two MVPN Gateway servers constitute an MVPN Service Group that follows an ACTIVE-STANDBY pattern. The goal is to substitute a failed MVPN server node as soon as possible and provide access to the same agency resources. Local redundancy assumes the usage of two instances of a physical hardware server in a single location.

In a Geo-Redundancy mode, two independent MVPN clusters work in an ACTIVE-ACTIVE pattern to provide simultaneous access to several geographically separated site locations. The client device can access resources in alternative agency sites if primary agency site has been compromised or disabled.

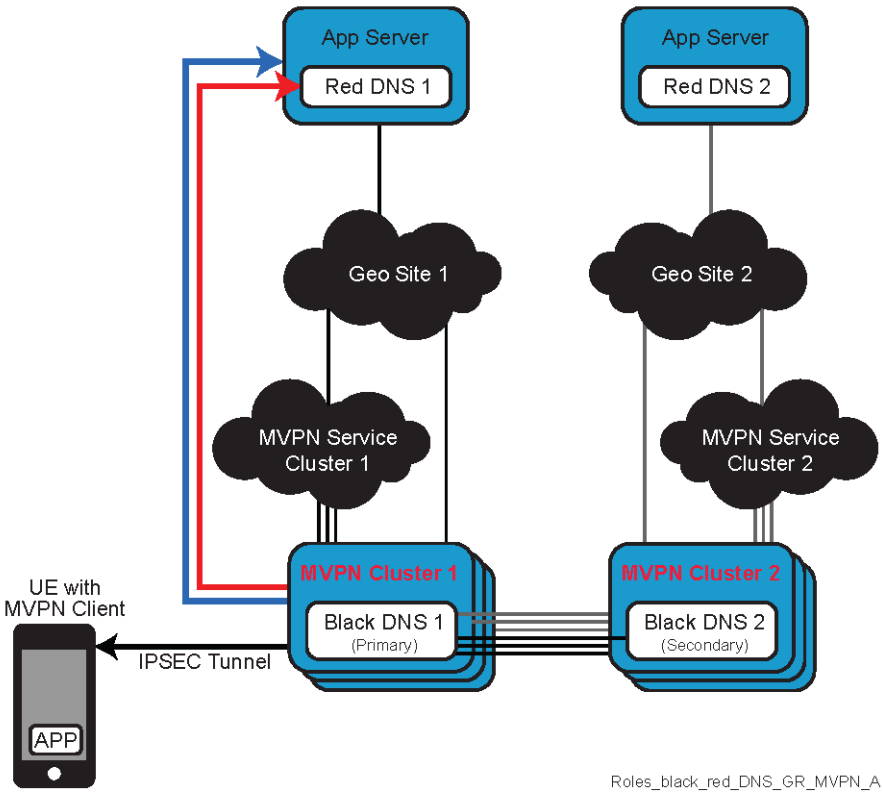
MVPN Gateway clusters in a Geo-redundancy configuration, do not share common configuration or synchronization. Each of the MVPN clusters works independently from each other. For an MVPN client UE device, each instance of a Geo-redundant MVPN cluster provides the same method of authentication, though the provisioning configuration such as RED DNS and IP pools are Geo-site specific. Applications working on client UE are expected to modify behavior and use resources located in a new geographical site.

Geo-redundancy assumes usage of one instance of the physical hardware server per each location for non-locally-redundant cluster (total 2) or two instances of a physical hardware server per each location for locally-redundant cluster (total 4). An increased number of physical servers working in ACTIVE-ACTIVE mode do not increase maximal client capacity. The overall capacity remains the same if one of the MVPN geo-redundant clusters is disabled.

1.9.2
MVPN and DNS Features

In the PSLTE 11 release, network design introduces two types of DNS servers - BLACK and RED DNS. Each type of DNS server has its own purpose and location. Geo-Redundant solution combines usage of MVPN Gateway and RED/BLACK DNS together to provide a necessary level of configuration management and control.

Figure 2: BLACK and RED DNS Architecture



NOTICE: Only floating external (public access) IP addresses of existing configured service groups should be provisioned for BLACK DNS record.

NOTICE: Each service group (which IP is added to A DNS record) must provide the same level of service to clients. Every service group should provide a profile with the same network permissions, VPN characteristics (either rekey or key lifetime), and authentication.

1.9.2.1
Black DNS

The BLACK DNS permits the MVPN client to choose the address of one of the available MVPN gateways. The algorithm-based selection of the MVPN gateway (from the list of many) provides extra level of failure resistance and load balancing across all MVPN service groups in an MVPN cluster. The MVPN client must be configured with an IP address of one BLACK DNS (or two for Geo-Redundancy) to use this feature.

By default, the BLACK DNS is located in the EPC network. The BLACK DNS is configured with names pointing to an actual IP address of floating VPN EXT interfaces.

The BLACK DNS configures the MVPN Client with the FQDN of the MVPN Service Groups associated with the client profile. The FQDN resolves to the list of MVPN Service Group addresses to optimize for normal conditions. Upon failure, the client attempts to establish a tunnel with an available MVPN Gateway instance using addresses in the list. The active state for IPsec session cannot be synchronized across MVPN Gateway instances and clients re-initiate connections upon failure.

1.9.2.2
Red DNS

The RED DNS provides name resolution for application services located in the Secure Enclave/ Agency. The address of the RED DNS is provided by the MVPN Gateway as part of the IPsec provisional session configuration. The MVPN client receives different RED DNS server depending on the Geo location or profile.

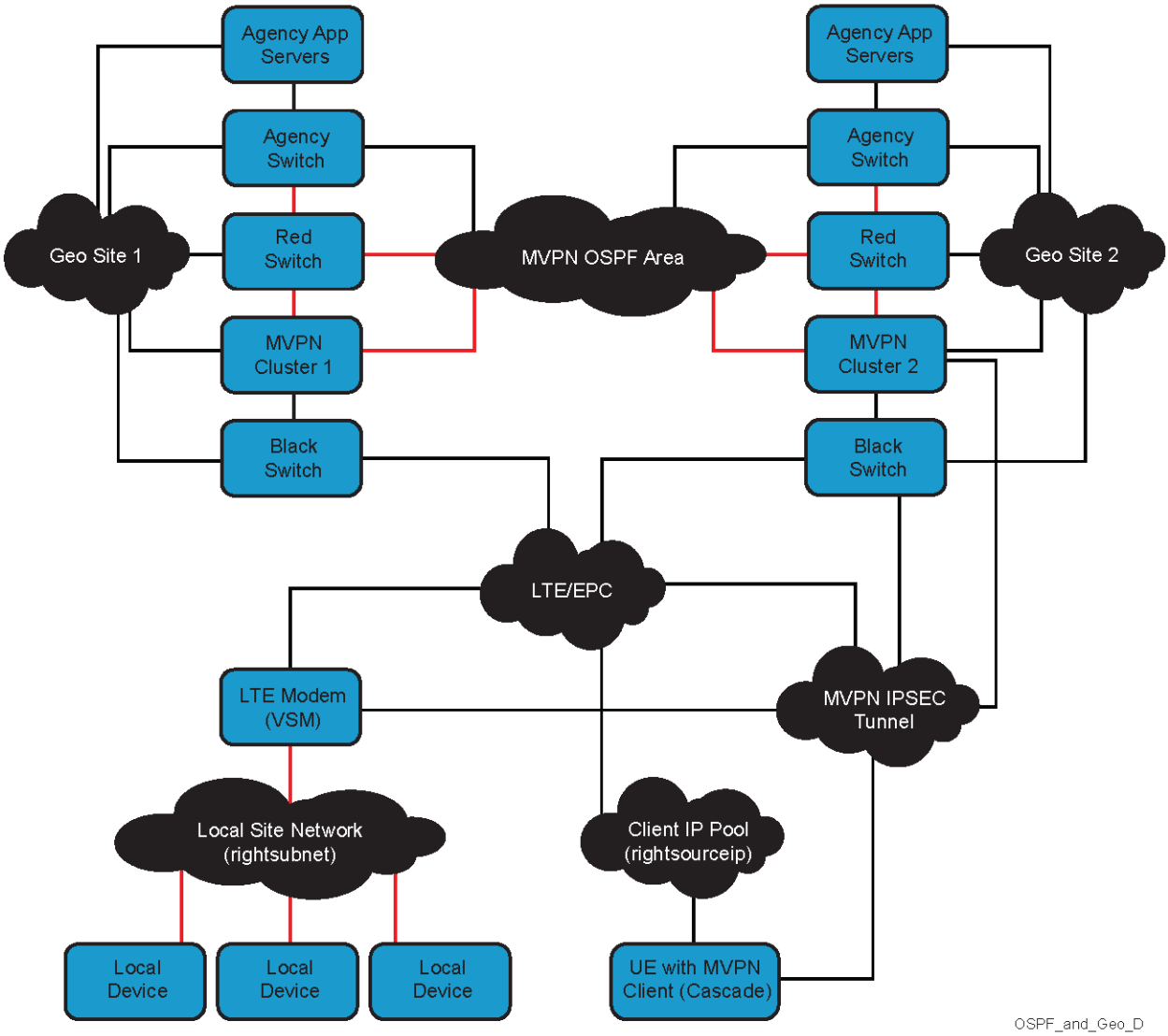
By default, the RED DNS is located in the Secure Enclave.

1.9.3
OSPF Features

An OSPF area configured by the MVPN gateway automatically sets the routing from the Secure Enclave to the UE destinations. A device using Site-to-Site OSPF profile seamlessly switches between different MVPN gateways with routing automatically updated. The OSPF feature requires:

- An adjacent RED switch
- Equipment connected to the RED switch to support OSPFv2
- MVPN OSPF area configured with the same authentication and parameters

Figure 3: MVPN OSPF



When designing customer-specific PSLTE solution involving MVPN OSPF, consider the following constraints:

- MVPN OSPF routing enables servers located in Agency and Secure Enclave to reach virtual VPN addresses of UE through proper MVPN Gateway.
- MVPN OSPF area spans from MVPN GW through RED Switch towards Agency and Secure Enclave.
- MVPN Gateway provides routing configuration to RED Switch when OSPF area is properly configured.

MVPN Gateway statically emits OSPF routing based on IPSEC profile data once "Remote Access OSPF" profile is created. The virtual VPN address pool (rightsourceip CIDR parameter of profile) is advertised as a subnet that is accessed through a local VPN INT address of the MVPN GW.

- Example: Local MVPN GW VPN INT address is 192.163.0.131. Profile rightsourceip CIDR is 10.2.0.0/26. Once a profile is created, OSPF routing sent to the RED SWITCH has a form "add route 10.2.1.0/26 via 192.163.0.131".

MVPN Gateway dynamically emits OSPF routing based on the state of IPSEC traffic selectors of the sessions established with a Site-to-Site OSPF profile. When the client and server negotiate IKEv2 session capabilities, they settle specification of subnets available on each side to define exact traffic selectors. Negotiated and approved subnets offered by Site-to-Site IPSEC client are advertised as subnets accessed through the local VPN INT address of the MVPN GW.

- Example: Local MVPN GW VPN INT address is 192.163.0.131. If the client offers subnet 10.1.1.0/24 and profile rightsubnet CIDR is 10.1.0.0/16, then the server approves client-side subnet 10.1.1.0/24. When IPSEC session is established, OSPF routing sent to the RED SWITCH has a form "add route 10.1.1.0/24 via 192.163.0.131".

1.9.3.1

Overview of OSPF Operational Characteristics of User Profiles

This section describes the operational OSPF related subnet differences (Site-to-Site subnets vs. Remote Access pools vs. Static areas). Rules for IP space separation for the MVPN Gateway are:

- Separation must exist between static and OSPF Virtual Private Network client subnets.
- Separation must exist within OSPF Virtual Private Network client subnets. OSPF subnets for Site-to-Site and OSPF subnets for Remote Access must be separated.

Table 4: OSPF Subnet Related Differences

Client Type	OSPF / Geo-Redundancy Environment	Non-OSPF Environment	Definition of client network	Interaction between MVPN GW and OSPF area
VSM (router mode)	OSPF Site To Site	Site to Site	Client subnet is static. The “**rightsubnet**” parameter must include all subnets from all VSM devices in use by the customer for the Mobile VPN Gateway.	Specific for device instance, OSPF route is propagated when the tunnel between the Mobile VPN Gateway and VSM is active.
UE with MVPN client (LEX, Cascade) 2. VSM (NAT mode)	OSPF Remote Access	Remote Access	Subnet (“**rightsourceip**” address pool) is unique for each Mobile VPN Gateway service group (globally).	OSPF route for subnet pool is propagated once profile added and when gateway node is active.

Chapter 2

Mobile VPN Gateway Installation

This chapter provides information and procedures to set up (install and configure) the Mobile VPN Gateway Server.

The Motorola Solutions Mobile VPN Gateway Server is an HP DL380 Virtual Management Server (VMS) host platform with (one or more) Virtual Machines used to provide Mobile VPN Gateway service.

Initial setup of the VMS host to support the Mobile VPN Gateway Server is established by installing the ESXi Operating System (OS) on the DL380 hardware platform and installing virtual machines. The image of the virtual machines, containing the Mobile VPN Gateway Server applications, is provided by Motorola Solutions. When the machines are installed, they require configuration.

2.1 Installing and Configuring the Mobile VPN Gateway Servers

Install and configure a new or replacement MVPN Gateway server:

- **For a new installation**, the server is pre-loaded with RAID, BIOS, iLO firmware, and VMware ESXi at the factory. Follow instructions in this process to check and skip or perform the pre-loaded steps.
- **For server hardware replacement in the field**, follow all the steps in this process. Contact your Motorola service representative to determine if the server replacement hardware is set up the same as a new server.

Prerequisites:
Obtain and install:

- Extreme x460 or equivalent switches
- NTP server

Obtain the HP DL380 Gen9 server.

Table 5: Components Within the Public Safety Mobile Virtual Private Network Gateway

Quantity	Component
1 (for non-redundant configuration)	DL380 Gen9 Server
2 (for redundant configuration)	DL380 Gen9 Server

Obtain:

- *Mobile Virtual Private Network Server Application* DVD
- *VMware ESXi Installation Media*
- *VMware vSphere Configuration Media*

IMPORTANT: The vSphere Client and the ESXi host server are designed to work together. A mismatch of the related releases can cause unexpected results.

Process:

1. Set up the DL380 Gen 9 host hardware.

   See Mobile Virtual Private Network Gateway Hardware Installation Process on page 42.

2. **For a new installation:** Set up the hardware platform for the Mobile VPN Server.

See Bare-Metal Setup of HP ProLiant DL380 Gen9 Servers on page 153.

3 Set up VMware ESXi:

   a Install ESXi.

   See Installing ESXi on page 48.

   b Perform initial ESXi Configuration.

   See Initial ESXi Configuration on page 49.

   c Customize the ESXi Server for the Mobile VPN Gateway.

   See Customizing ESXi Server for Mobile VPN Gateway on page 51.

4 Log in to the VMware vSphere Client.

   See Logging On to the VMware vSphere Client on page 53.

5 Import OVF into the Virtual Server.

   See Importing OVF into Virtual Server on page 55.

6 Verify import of the OVF into the Virtual Server.

   See Verifying Import of the OVF into Virtual Server on page 57.

7 Set the Mobile VPN virtual machine startup and shutdown order.

   See Setting the Mobile VPN Virtual Machine Startup and Shutdown Order on page 57.

8 Apply Virtual Machine supplemental configuration.

   See Applying Virtual Machines Supplemental Configuration on page 58.

9 Configure Virtual Machine security settings.

   See Configuring Virtual Machine Security Settings on page 61.

10 Configure Virtual Machine resource settings.

   See Configuring Virtual Machine Resource Settings on page 62.

11 Upgrade VMware Tools on Linux-based Virtual Machines.

   See Reconfiguring VMware Tools on Linux-Based Virtual Machine on page 63.

12 Configure the Network Identity.

   See Configuring the Network Identity on page 65.

13 Repeat "step 5" through "step 14" for each virtual machine required. Use the same OVF file from the *Mobile Virtual Private Network Application* DVD to create each additional virtual machine. Ensure to enter a different name in the virtual machine **Name** field each time you repeat the procedure.

   The number of virtual machines required depends on the Mobile VPN Gateway licensing that your organization purchased.

   Continue with the next step.

14 Perform the following procedures from the Mobile VPN Gateway Configuration on page 61 chapter:

   NOTICE: Perform all steps for each virtual machine, unless otherwise noted.

   a Define the cluster.

   See Defining the Cluster on page 72.

   b Optional: Add a Service Group to the cluster.

   See Adding a Service Group to the Cluster on page 75.

c **For the service group hierarchical level:** apply a license to a Virtual Machine.

See Licensing Administration on page 70.

d Manage routing.

See Managing Static Routing on page 79.

e If the client authentication is planned to be performed using Active Directory, continue with Setting Up MVPN Server to Client Authentication Including Active Directory on page 96 and return here.

f Set system time.

See System Time on the Mobile VPN Gateway on page 68.

g Optional: Join the Mobile VPN Gateway to an existing Domain Controller.

See Joining the Mobile VPN Gateway to an Existing Domain Controller on page 67.

h Manage the Centralized Syslog Client configuration.

See Managing Centralized Syslog Client Configuration on page 70.

NOTICE: "Step 16i" and "Step 16j" are part of Device Authentication Method Configuration on page 88.

i Manage certificates.

See:

1. Generating the Certificate Signing Request on page 88
2. Importing the Certificate Chain on page 90

j **For the cluster hierarchical level:** manage pre-shared keys.

See Adding Pre-Shared Keys for ASTRO Subscriber on page 93.

k **For the service group hierarchical level:** create connection profiles.

See Creating Connection Profiles for the Mobile VPN Gateway on page 101.

l **For the service group hierarchical level:** add authentication to a profile.

See Adding Authentication to a Profile on page 108.

m Add a bypass configuration.

See Adding a Bypass Configuration on page 84.

n Optional: Verify and change the gateway node status in High Availability Administration on page 118, if needed.

o Optional: **For the cluster hierarchical level:** set the statistics logging configuration.

See Setting the Statistics Logging Configuration on page 129.

Postrequisites:
For each additional virtual machine that must be installed on a host platform that is already configured, repeat “Installing and Configuring the Mobile VPN Gateway Servers” for each virtual machine, starting from "Step 4".

For a secondary server, repeat “Installing and Configuring the Mobile VPN Gateway Servers” starting from "Step 1".

2.1.1
Mobile Virtual Private Network Gateway Hardware Installation Process

The following is the list of procedures for installing the hardware for the Public Safety LTE Mobile Virtual Private Network Gateway system.

Process:

1. Unpack and mount all hardware components in the rack. For instructions on unpacking and mounting HP ProLiant DL380 Gen9 servers component rack, see the following third-party vendor documentation:
   - *HP ProLiant DL380 Gen9 Server User Guide* at http://www.hp.com/go/docs (select **Gen9** → **DL380**)
   - *HP Quick Deploy Rail System Installation Instructions* (ships with product)

   CAUTION: Ensure that the site is correctly prepared for the installation and that all environmental, installation, health and safety, operational space, and electrostatic discharge safety requirements described in the appropriate third-party vendor documentation are met.
2. See Connector Locations and Cabling on page 43.
   a. See Mobile Virtual Private Network Gateway Connector Locations and Cabling on page 43.
   b. Perform Connecting Optional Monitor and Keyboard with HP DL380 Server on page 47.
3. Perform Virtual Private Network Gateway Power On Startup Sequence on page 48.

2.1.2
HP DL380 Gen9 Servers

The HP ProLiant DL380 Gen9 (HP DL380 Gen9) is used in the network for the Mobile VPN Gateway.

Within the server, both a database and user applications interface are available.

NOTICE: The front view photo shows a typical HP DL380 Gen9 server. The configuration varies dependent upon the network element in the network.

Figure 4: Typical HP DL380 Gen9 Server (General)

For detailed information on the HP DL380 Gen9 server and technical specifications, see the most up-to-date documentation. This is the vendor documentation included in the shipment, or the manuals for the HP ProLiant DL380 Gen9 Server retrieved from http://h17007.www1.hp.com/docs/enterprise/servers/DL380Gen9/DL380Gen9-setup/system_setup_overview/setup.htm and http://h20565.www2.hpe.com/hpsc/swd/public/readIndex?sp4ts.oid=7271242.

For Setup Overview of the server, see http://h20565.www2.hpe.com/portal/site/hpsc/public/psi/manualsResults?sp4ts.oid=7271241.

For more information on the size of Field Replaceable Units (FRUs) hard drives for servers and associated equipment, see Mobile VPN Gateway FRU/FRE Information on page 151. Note that hard disks are labeled with specifications on the front of the drive.

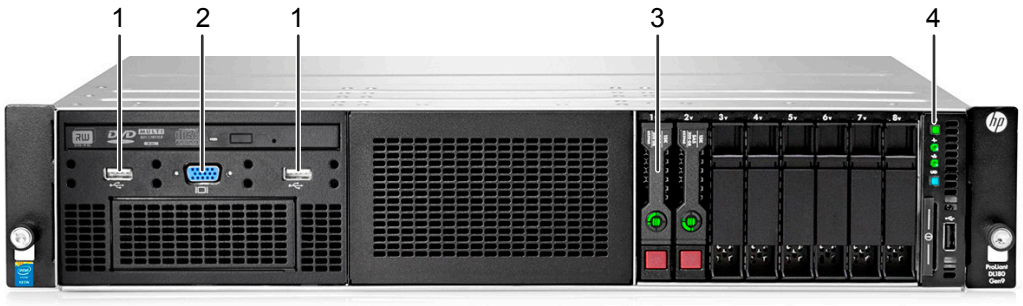
2.1.3
Connector Locations and Cabling

The following figures and tables, along with the IP Plan unique to your system, can help you connect the Ethernet cabling between the components.

2.1.3.1
Mobile Virtual Private Network Gateway Connector Locations and Cabling

The figures and tables provide the location and designations of the Ethernet connectors on the rear of the server chassis. For the Motorola Solutions virtual server implementations, the zero-based physical NIC labeling applied over the HP labeling, aligns with the zero-based default VMware virtual interface numbering.

Figure 5: Mobile VPN Gateway DL380 – Front View



hpdl380gen9_mvpn_pslte_front

Table 6: Mobile VPN Gateway DL380 Front View Annotations

Annotations	Description
1	USB Ports for Keyboard and Mouse
2	Video Connector
3	SFF Drive Bay **NOTICE:** Mobile VPN Gateway is equipped in two drives.

Table continued…

Annotations	Description
4	Power On/Standby button and system power LEDs (Health LED, NIC status LED, UID button)

Figure 6: Mobile VPN Gateway DL380 – Rear View

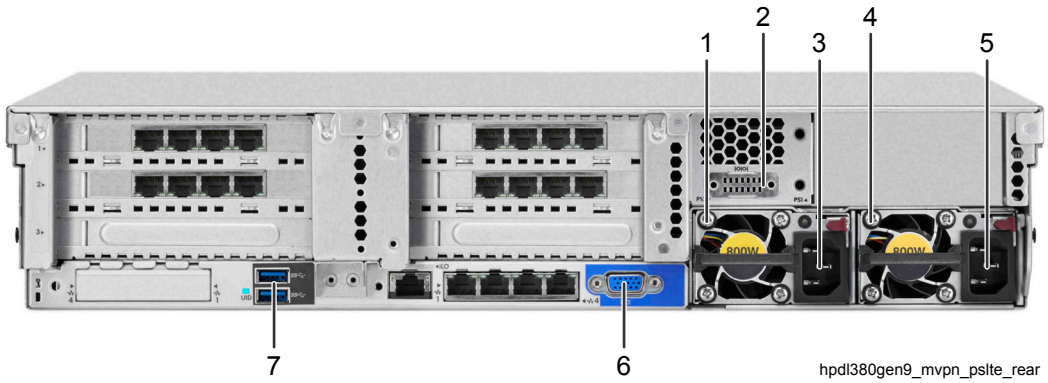
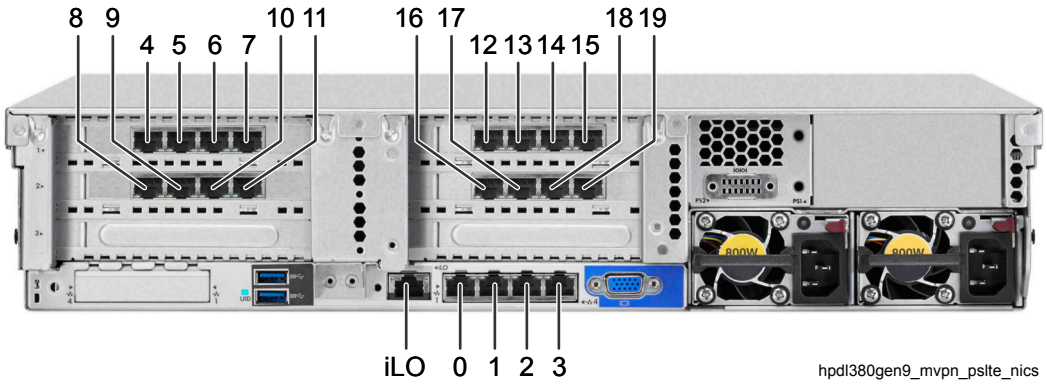


Table 7: Mobile VPN Gateway DL380 Rear View Annotations

Annotations	Description
1	Power Supply 1
2	Serial Connector
3	PS 1 Power Connector
4	Power Supply 2
5	PS 2 Power Connector
6	Video Connector
7	USB Connectors

Figure 7: Mobile VPN Gateway DL380 – NIC ports



NOTICE: The numbers annotated in this picture represent NIC port numbers.

The virtual machine numbering for the Ethernet ports on a Mobile VPN Gateway are shown in "Figure 5: Mobile VPN Gateway DL380 - NIC Ports". Ports correspond to "Table 6: Cable Connections for Mobile Virtual Private Network Gateway (Redundancy Example)" which is an example of Mobile VPN Gateways in the redundant configuration of a Motorola-defined “Multi-Solution Subsystem” reference architecture. See your customer specific IP Planner unique to your system.

Contact your Motorola Solutions service representative for more information about the network elements in the “To” column for your system.

In this example of a redundant configuration:

- VPN 1 represents the HP DL380 where the vCenter virtual machine is initially installed.
- VPN 2 represents the HP DL380 where the Mobile VPN Gateway virtual machines are initially installed.

Table 8: Cable Connections for Mobile Virtual Private Network Gateway (Redundancy Example)

From	Type	To	Connector
iLO port, VPN 1		Network L2-L3 Switch/Router (Primary)	Site Dependent
iLO port, VPN 2		Network L2-L3 Switch/Router (Redundant)	Site Dependent
NIC 0, VPN 1	RJ45/Ethernet	Network L2-L3 Switch/Router (Primary)	Site Dependent
NIC 0, VPN 2	RJ45/Ethernet	Network L2-L3 Switch/Router (Redundant)	Site Dependent
NIC 1, VPN 1	RJ45/Ethernet	Network L2-L3 Switch/Router (Redundant)	Site Dependent
NIC 1, VPN 2	RJ45/Ethernet	Network L2-L3 Switch/Router (Primary)	Site Dependent
NIC 2	RJ45/Ethernet	Not used.	

Table continued…

From	Type	To	Connector
NIC 3	RJ45/Ethernet	Not used.	
NIC 4,VPN 1	RJ45/Ethernet	Network L2-L3 Switch/Router (Primary)	Site Dependent
NIC 4,VPN 2	RJ45/Ethernet	Network L2-L3 Switch/Router (Redundant)	Site Dependent
NIC 5, VPN 1	RJ45/Ethernet	Network L2-L3 Switch/Router (Primary)	Site Dependent
NIC 5, VPN 2	RJ45/Ethernet	Network L2-L3 Switch/Router (Redundant)	Site Dependent
NIC 6, VPN 1	RJ45/Ethernet	Network L2-L3 Switch/Router (Primary)	Site Dependent
NIC 6, VPN 2	RJ45/Ethernet	Network L2-L3 Switch/Router (Redundant)	Site Dependent
NIC 7	RJ45/Ethernet	Not used.	
NIC 8, VPN 1	RJ45/Ethernet	Network L2-L3 Switch/Router (Redundant)	Site Dependent
NIC 8, VPN 2	RJ45/Ethernet	Network L2-L3 Switch/Router (Primary)	Site Dependent
NIC 9, VPN 1	RJ45/Ethernet	Network L2-L3 Switch/Router (Redundant)	Site Dependent
NIC 9, VPN 2	RJ45/Ethernet	Network L2-L3 Switch/Router (Primary)	Site Dependent
NIC 10, VPN 1	RJ45/Ethernet	Network L2-L3 Switch/Router (Redundant)	Site Dependent
NIC 10, VPN 2	RJ45/Ethernet	Network L2-L3 Switch/Router (Primary)	Site Dependent
NIC 11	RJ45/Ethernet	Not used.	
NIC 12, VPN 1	RJ45/Ethernet	Network L2-L3 Switch/Router (Primary)	Site Dependent
NIC 12, VPN 2	RJ45/Ethernet	Network L2-L3 Switch/Router (Redundant)	Site Dependent
NIC 13, VPN 1	RJ45/Ethernet	Network L2-L3 Switch/Router (Primary)	Site Dependent
NIC 13, VPN 2	RJ45/Ethernet	Network L2-L3 Switch/Router (Redundant)	Site Dependent
NIC 14	RJ45/Ethernet	Not used.	
NIC 15	RJ45/Ethernet	Not used.	
NIC 16, VPN 1	RJ45/Ethernet	Network L2-L3 Switch/Router (Redundant)	Site Dependent
NIC 16, VPN 2	RJ45/Ethernet	Network L2-L3 Switch/Router (Primary)	Site Dependent

Table continued…

From	Type	To	Connector
NIC 17, VPN 1	RJ45/Ethernet	Network L2-L3 Switch/Router (Redundant)	Site Dependent
NIC 17, VPN 2	RJ45/Ethernet	Network L2-L3 Switch/Router (Primary)	Site Dependent
Serial Port	RS-232	Not used.	Not used.
USB ports	USB v2.0 and 1.1 compliant	Not used.	Site Dependent / Optional.
Video port	VGA/HD15	Monitor	Site Dependent / Optional.
Mouse connector	USB ports for installation / configuration	Mouse	Site Dependent / Optional.
Keyboard connector	USB ports for installation / configuration	Keyboard	Site Dependent / Optional.

2.1.3.2

Connecting Optional Monitor and Keyboard with HP DL380 Server

This section describes the connection for the optional monitor and keyboard with the HP DL380 Server.

Prerequisites: Ensure that the HP DL380 servers, an optional keyboard, and monitor are mounted on the same rack. The keyboard and monitor components are optional. Use a rack installed model to have direct local access to the server.

When and where to use:
Cabling these connections aids in supporting/monitoring any future server configurations.

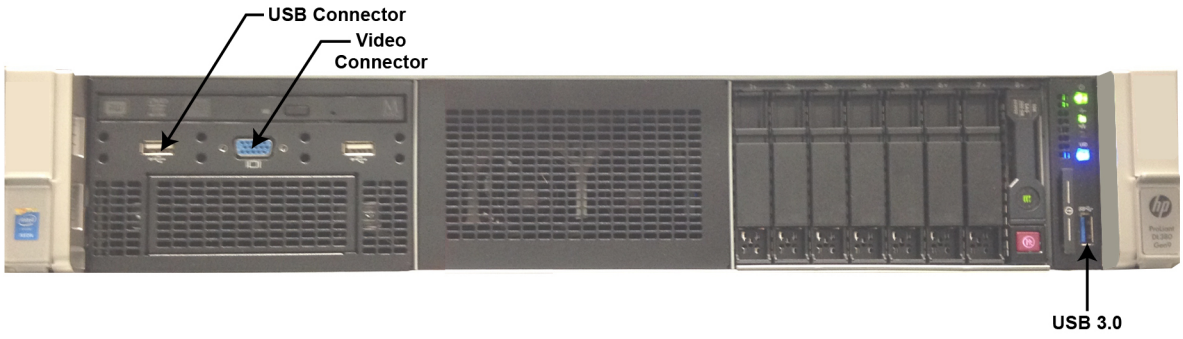
Perform the following procedure to cable the connection between a VGA monitor, keyboard, and one of the HP DL380 servers.

Procedure:

1 Locate the VGA port (shown as the Video Connector in the figure) on the HP DL380 server front panel.

The video port interface is a standard VGA compatible, 15-pin connector. This port is also available at the rear of the server.

Figure 8: HP DL380 Gen9 Server Front Panel — Monitor and Keyboard Connectors



HP_DL380_Gen9_Server_front2_B

See Figure 5: Mobile VPN Gateway DL380 – Front View on page 43.

2. Connect the VGA monitor cable to the desired server.
3. Locate an unused USB port (shown as the USB connector in the figure) on the HP DL380 server front panel.

   The USB port interface is a standard USB connector. USB ports are also available at the rear of the server.
4. Connect the keyboard cable to the (same) desired server.

2.1.4
Virtual Private Network Gateway Power On Startup Sequence

This section describes the power-on and initialization procedures of the hardware components.

Prerequisites:

NOTICE: Before powering on the components, ensure that all site power and grounding requirements as described in Mobile Virtual Private Network Gateway Hardware Installation Process on page 42 are met.

When and where to use:
Main power to the rack may be connected to a single, primary source of power, or to two sources of power for redundancy. Two circuit breakers are typically used in redundant configurations. When applying main power to the rack, before powering on the components, ensure that all main power source circuit breakers are turned on.

Procedure:

1. Apply main power to the rack.
2. Turn on the power distribution unit (PDU) circuit breakers to apply power to the rack.
3. Power on the optional rack mounted keyboard and monitor (if used).
4. Power on any routers or switches.
5. Power on the server.

2.2
Mobile VPN Gateway VMware ESXi Setup

Perform procedures in this section to set up the Mobile VPN Gateway VMware ESXi.

2.2.1
Installing ESXi

This procedure installs the ESXi server.

Procedure:

1. When prompted to select the **Boot Menu**, press `F11`.
2. Insert the VMware ESXi installation media into the optical drive.
3. At the prompt that appears, press the number corresponding to the `CD-ROM`.
4. In the VMware ESXi boot menu, use the arrow keys to select the `Installer` and press ENTER.

   If no option is selected, the installer option will automatically be selected after 10 seconds.
5. At the prompt that appears after the installer finishes loading, press ENTER.

6 When the **End User License Agreement** is displayed, press `F11` to accept it.

A list of storage devices displays.

7 Under **Local**, use the arrow keys to select `LUN 00` or `Internal SD-Card`. Press ENTER.

The device capacity is approx. 8GB.

8 **Only for systems with previously installed ESXi:** Perform one of the following actions:

If…	Then…
If the device selected for installation contains data,	in the confirmation message, press ENTER.
If the device selected for installation previously contained a VMware ESXi installation,	this is a version update, use the arrow keys and spacebar to select `Install` and press ENTER.

9 At the keyboard layout dialog, select `US Default` for the keyboard input. Press ENTER.

10 Enter the system `root` password twice.

IMPORTANT: Do not use the special character “&” in the password. This will cause scripts to fail.

11 At the **Confirm Install** dialog, press `F11`.

12 When the Installation Complete message displays, press ENTER to reboot.

The server reboots, initializes, and displays the **VMware ESXi** screen.

2.2.2
Initial ESXi Configuration

This procedure configures the administrator password, network interface settings, and troubleshooting mode options for the VMware ESXi hypervisor on the Application Server.This procedure configures the administrator password, network interface settings, and troubleshooting mode options for the VMware ESXi hypervisor on the Mobile VPN Gateway Server.

Prerequisites:
Ensure that a VGA monitor, a keyboard, and a mouse are connected to the Mobile VPN Gateway Server.

Procedure:

1 Press any key to wake up the system.

2 Access the VMware ESXi Direct Console User Interface (DCUI):

- **a** Press F2.
- **b** At the authentication prompt, in the **Login Name** field, enter `root`

3 Configure the administrator password:

- **a** At the **System Customization** screen, select **Configure Password**.
- **b** At the **Configure Password** screen, leave the **Old Password** field blank.
- **c** In the **New Password** field, enter: ***<new password>***
- **d** In the **Confirm Password** field, re-enter the ***<new password>***.
- **e** Save your changes by pressing ENTER.

4 Configure the management network:

NOTICE: Enter the appropriate values for the IP Address, Subnet Mask, and Default Gateway according to the *System IP Plan*.

a At the **System Customization** menu, select **Configure Management Network**.

b From the **Configure Management Network** menu, select **IP Configuration**.

c At the **IP Configuration** screen, select the **Set static IP address and network configuration** radio button with the spacebar.

d In the **IP Address** field, enter: ***<Agency network prefix [a.b.c]>.<xyz>***

where:

<Agency network prefix> is the first three octets, which are part of IP planning and commissioning data

<a>, ***<b>***, and ***<c>*** variables are numbers between 0–255

<xyz> is 4-th octet value of physical ESXi server IP address according to System IP Plan. Default values are `144` for the primary ESXI vpngw1 server and `146` for the redundant ESXI vpngw2 server.

e In the **Subnet Mask** field, enter `255.255.255.128`

f In the **Default Gateway** field, enter: ***<Agency network prefix [a.b.c]>.<xyz>***

where:

<Agency network prefix> is the first three octets, which are part of IP planning and commissioning data

<a>, ***<b>***, and ***<c>*** variables are numbers between 0–255

<xyz> is is the Gateway IP address as stated in the *System IP Plan*

g Save your changes by pressing ENTER.

h At the **Configure Management Network** menu, press ESC.

i When prompted whether to apply changes and restart the management network, press Y.

5 Configure DNS for ESXi:

a At the **System Customization** menu, select **Configure Management Network**.

b From the **Configure Management Network** menu, select **DNS Configuration**.

c At the **DNS Configuration** screen, select the **Use the following DNS server addresses and hostname** radio button with the spacebar.

d In the **Primary DNS Server** field, enter appropriate value for **Primary DNS Server**.

e In the **Alternate DNS Server** field, enter appropriate value for **Alternate DNS Server**.

f Save your changes by pressing ENTER.

6 Set troubleshooting options:

a At the **System Customization** menu, select **Troubleshooting Options**.

b At the **Troubleshooting Mode Options** menu, verify that the **ESXi Shell** and **SSH** options are enabled.

If either one of those options is disabled, select the disabled item and press ENTER to toggle the setting between `Enabled` and `Disabled`.

7 Press ESC twice.

8 Disconnect the keyboard, mouse, and monitor.

2.3

Customizing ESXi Server for Mobile VPN Gateway

This procedure allows you to customize the ESXi server.

Prerequisites:

- Obtain *VMware vSphere Configuration Media*.
- Ensure that the System IP Plan is available.
- Install PowerCLI on the Windows device.
- PuTTY application suite is loaded on the Windows device. The directory containing PuTTY software is added by PuTTY installer to PATH Windows system variable.

Procedure:

1. To disable the use of a proxy server, perform the following actions:
   a. From **Start**, navigate to **Control Panel** → **Network and Internet** → **Internet Options**.
      The **Internet Options** dialog box appears.
   b. Click the **Connections** tab.
   c. Click the **LAN Settings** button.
   d. Clear the box for **Use a proxy server for your LAN**.

   NOTICE: This setting does not apply to dial-up or VPN connections.
2. Insert the *VMware vSphere Configuration Media* in to the drive of the computer where the vSphere client resides.
3. On the Windows machine, right-click **PowerCLI** shortcut and select **Run As System Administrator**.
4. At the PowerCLI console, run the ESXi configuration script:
   a. Enter:
      `cd <VMware vSphere Configuration Media location>\common\bin\`
   b. Enter: `.\ConfigureESXIServer.ps1`

   where *<VMware vSphere Configuration Media location>* is the directory path that you can copy from the Microsoft Windows GUI after navigating to the `mot-csr-vsphere-cfg` directory

   Step example: `mot-csr-vspherecfg-xx.xx.xx-xx\`
   From the absolute path address shown on the top of the file folder window, you can right-click the arrow and select **Copy address**.

   `ConfigureESXIServer.ps1` prints the list of Identity Type choices and prompts for Identity Type.
5. Enter the configuration parameters according to your IP plan:
   a. At the `Identity` prompt, enter the number corresponding to `CEN`
   b. At the `Server Type` prompt, enter the number corresponding to the `VPN`
   c. Enter the `Start Vlan ID` (in multiples of 100 up to 3900) for the virtual port groups per IP plan

For example: provide the value `100`, when customer **OOBM VLAN ID** is globally configured with value `212`, which is sum of `Start VLAN ID` value and the default offset `112` for **OOBM VLAN** from System IP Plan.

d Enter the `ESXi Host Name` per IP plan.

By default, the hostname value is `vpngw1` for ESXI 1 server and `vpngw2` for ESXI 2 server.

e Enter the `ESXi Host IP` per IP plan.

f At the `Enter User Name` prompt, enter `root`

g Enter the appropriate password and confirm it.

If the entered IP and user credentials cannot be used to make a connection to the server, you are prompted to reenter the proper user name, password, and ESXi Host IP address.

h Enter the user account password for hafence and confirm it.

i Enter the `License Key` per manufacture sticker.

j Enter the number corresponding to the Local datastore.

k Enter the `Firewall Allowed IP Address(es) for SNMP`. If all IPs are allowed, click ENTER.

l If the Mobile VPN Gateway is supported by a remote syslog server, enter the syslog server IP

m Enter the number of syslog files before rotation, or press ENTER to accept default number.

n If the Mobile VPN Gateway is supported by an NTP server, enter the NTP server IP address as the time source.

o When asked if the server is an NTP Host, enter N

p Enter the date-time for this machine. Use local time zone. If the local PC current time is to be used, click ENTER.

The configured time for the ESXi server must be within 5 minutes of the time on the TRAK or NTP time synchronization cannot be successfully performed.

q Verify the parameters you entered.

r Perform one of the following actions:

To accept and apply the ESXi config changes, enter Y
To modify the entered values, enter M
To reenter all values, enter N
To quit, enter Q

After accepting the parameters, the script executes the below tasks to configure the ESXi server and prints the status of the executed tasks. Details such as version information in the user installation output can differ from the example provided here.

```
Setting the license key.
[ OK ]
Setting date-time.
[ OK ]
Configuring Firewall.
[ OK ]
Setting Local Datastore.
[ OK ]
Installing package esxcli-shell-x.x.x-xx-offline_bundle.zip.
[ OK ]
Restarting hostd.
[ OK ]
```

```
Setting syslog configurations.
[ OK ]
Setting the scratch partition parameters.
[ OK ]
Setting FaultManagement Parameters.
[ OK ]
Setting NTP Client Configurations.
[ OK ]
Configuring vSwitches.
[ OK ]
Setting portgroup(s) and virtual network adaptor(s)
[ OK ]
ConfigureESXiServer.ps1 run status
[ OK ]
Press enter to exit:
```

s When all tasks are done, press ENTER.

6 Perform one of the following actions:

If…	Then…
If the script runs successfully and tasks show status `[OK]`,	continue to step 7.
If the script fails,	check the **Event Viewer** for error messages: **a** In the Windows **Start menu**, in the search box, enter `event viewer` **b** In the **Event Viewer**, select **Windows Logs** → **Application** **c** In the **Application** event log, search the events with Source of `esxiconfig` and the events of Level `Error`. **d** Find the solution to the errors, then re-run this script again. **e** Continue to step 7

7 From the VMware vSphere client, select the server name/IP, right-click and select **Reboot**.

8 Log on to the server.

2.4 Logging On to the VMware vSphere Client

This section provides the procedure to follow to log on to the VMware vSphere Client.

Prerequisites:

- Install the vSphere client. See Installing the VMware vSphere Client on Windows-Based Computer on page 158.
- You have obtained the IP address and root user password of the ESXi host server.
- Connect the local machine using an Ethernet cable to a configured, working port on the HP DL380 server. Alternatively, connect to the local network if the server is configured and available on the local network.

When and where to use: This procedure describes how to log on to access the VMware vSphere Client.

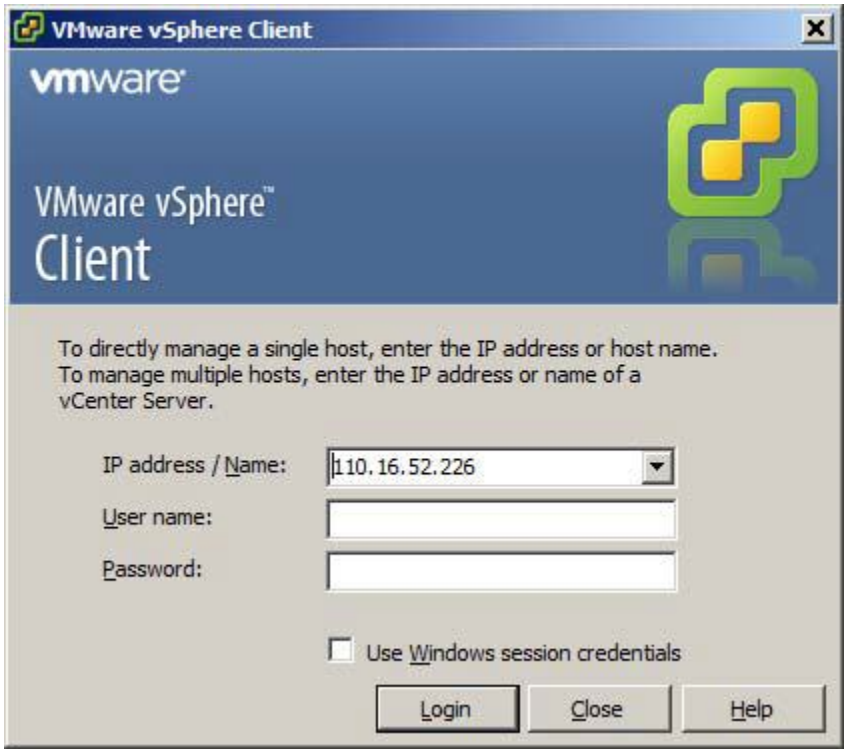
Procedure:

1 Launch the VMware vSphere Client from the Windows-based device (local machine) on which it resides. You can use **Start** → **Programs** or a desktop shortcut.

NOTICE: At the initial installation, a desktop shortcut was automatically created.

A dialog box appears and prompts for an IP address, user name, and password.

Figure 9: VMware Sphere Client Login Screen



2 Perform the following:

a Enter the IP address of the ESXi server.

b Enter the user name `root`

c Enter the root user password of the ESXi server.

d Click **Login**.

Either of the following may occur:

- If this is not a first-time login, the vSphere **Client Home** window appears. Go to step 4.
- If this is a first-time login, a **Security Warning** window appears displaying Certificate Warnings.

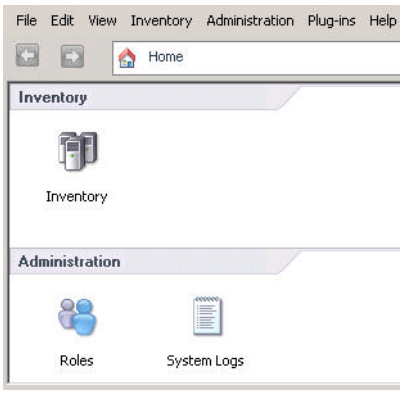
3 In the **Security Warning** window, perform the following:

a Mark the check box for **Install this certificate and do not display any security warnings**.

b Select **Ignore**.

NOTICE: Subsequent system procedures assume that you performed this step, so that the **Security Warning** window will no longer display after you log in.

Figure 10: vSphere Client Main Window – Home

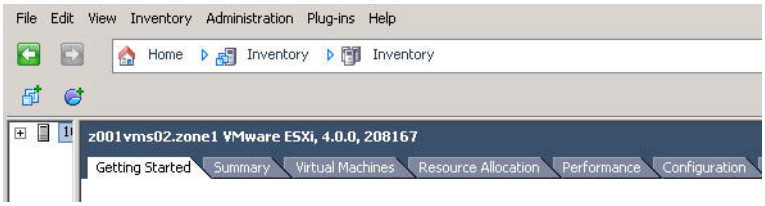


The vSphere **Client Home** window appears, and the IP address of the ESXi server appears in the title bar of the window.

4 Click the **Inventory** icon in the vSphere **Client Home** window.

NOTICE: Subsequent system logins and procedures assume that the top-level Home screen will no longer display after you log in. Instead, the vSphere **Client Inventory** window appears.

Figure 11: vSphere Client – Getting Started Tab



The vSphere **Client Inventory** window appears, with the Getting Started tab active. The ESXi server is selected from the navigation tree on the left side of the screen.

A successful login to the vSphere client is performed. Subsequent system logins result with the vSphere **Client Inventory** window displayed.

2.5 Importing OVF into Virtual Server

Procedure:

1 Launch the VMware vSphere Client from the Windows-based device (local machine) on which it resides. You can use **Start** → **Programs** or a desktop shortcut.

NOTICE: At the time of initial installation a desktop shortcut was automatically created.

A dialog box appears prompting for an IP address, user name, and password.

2 Perform the following actions:

a Enter the IP address of the ESXi server.

b Enter the user name `root`

c Enter the root user password of the ESXi server.

d Click **Login**.

The vSphere **Client Inventory** window appears.

3 In the DVD drive of the Windows Machine where the vSphere Client resides, insert the **Mobile Virtual Private Network Gateway Application DVD**.

4 From the **File** menu in the vSphere Client, select **Deploy OVF Template**.

5 In the **Deploy OVF Template** window, click **Browse**.

The **Deploy OVF Template** window displays file directories.

6 Navigate to the virtual machine files on the DVD **VPNGW-LTE*<version number>*** → **VPNGW-LTE-*<version number>*.ovf** and click **Open**.

The file name and path for the virtual machine you selected appear on the **Deploy OVF Template** window.

7 Click **Next**.

The **OVF Template Details** screen appears in the **Deploy OVF Template** window.

8 Click **Next**.

The **Name and Location** screen appears in the **Deploy OVF Template** window.

9 In the **Name** field, change proposed name of virtual machine to the format `<Hostname Prefix>vpngw<Application ID>`, then click **Next**.

Where:

- ***<Hostname Prefix>*** is based on the hostname definitions in IP plan of your system.
- ***<Application ID>*** is a single digit 1-8.

NOTICE: Each time the procedure is repeated, in the **Name** field, enter a different virtual machine name.

NOTICE: The procedure Configuring the Network Identity on page 65 for given virtual machine shall use same ***<Hostname Prefix>*** and ***<Application ID>*** values.

10 In the **DataStore** list, select the appropriate datastore for Virtual Machine Deployment and click **Next**.

NOTICE: This step is only applicable if multiple datastores are configured.

11 In the **Disk Format** screen, select the **Thick-provisioned, eager zero** option and click **Next**.

12 In the **Network Mapping** screen, from the **Destination Networks** drop-down list, select the appropriate **Network Label** for the virtual machine and click **Next**. Use the following table to select the appropriate labels.

Table 9: Network Mapping

Application	Source Network vpnint1 – Network Label	Source Network vpnext1 – Network Label	Source Network vpnha1 – Network Label	Source Network mgmt0 – Network Label
vpngw1	vpnint1	vpnext1	vpnha1	mgmt0
vpngw2	vpnint1	vpnext1	vpnha1	mgmt0

Table continued…

Application	Source Network vpnint1 – Network Label	Source Network vpnext1 – Network Label	Source Network vpnha1 – Network Label	Source Network mgmt0 – Network Label
vpngw3	vpnint2	vpnext2	vpnha1	mgmt0
vpngw4	vpnint2	vpnext2	vpnha1	mgmt0
vpngw5	vpnint3	vpnext3	vpnha2	mgmt0
vpngw6	vpnint3	vpnext3	vpnha2	mgmt0
vpngw7	vpnint4	vpnext4	vpnha2	mgmt0
vpngw8	vpnint4	vpnext4	vpnha2	mgmt0

13 In the **Ready to Complete** window, verify the displayed information, then click **Finish**.

The deployment of the virtual machine can take from 10 to 20 minutes.

The **Deploying...** window appears showing the progress of the deployment.

14 When the **Completed successfully** message appears, click **Close**.

The virtual machine import is completed.

15 Remove the **Mobile Virtual Private Network Gateway Application DVD** from the DVD drive.

2.6 Verifying Import of the OVF into Virtual Server

Prerequisites: Log in to the VMware VSphere Client, see Logging On to the VMware vSphere Client on page 53

Procedure:

Verify that the left pane of the vSphere Client main window displays the virtual machine name that you entered in "Step 9" Importing OVF into Virtual Server on page 55.

You may need to expand the list in the left pane to locate the virtual machine name.

2.7 Setting the Mobile VPN Virtual Machine Startup and Shutdown Order

Virtual machines hosted on a Virtual Management Server (VMS) are configured to boot automatically with the system in a prescribed order. When you install a virtual machine on a VMS, change the VMS settings to ensure that the new virtual machine boots in the correct order with respect to the other virtual machines hosted on the VMS.

Procedure:

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

A desktop shortcut was created during installation.

2 Log on to the server as `root`.

3 On the upper left side of the **vSphere Client Inventory** window, select the ESXi server.

4 On the right side of the window, select the **Configuration** tab.

The window displays information about the configuration of the ESXi server.

5 In the **Software** section, select **Virtual Machine Startup/Shutdown**.

6 On the right side of the main window, select **Properties**.

7 In the **System Settings** area, select **Allow virtual machines to start and stop automatically with the system**.

8 In the **Default Startup Delay** area, select **Continue immediately if the VMware Tools start**.

9 In the **Default Shutdown Delay** area, from the **Shutdown Action** drop-down list, select **Guest Shutdown**.

10 Set the virtual machines hosted on the ESXi server to be booted in any order:

   a In the **Startup Order** area, from the **Automatic Startup** list, select a virtual machine.

   b Move the virtual machine to the **Any Order** area by clicking the **Move Up** and/or **Move Down** buttons.

11 Repeat step 10 for each VM on the server.

12 Click **OK**.

   The **Properties** window closes.

2.8 Applying Virtual Machines Supplemental Configuration

Virtual machines hosted on the ESXi-based Virtual Management Server (VMS) require supplemental configuration to improve their security settings. You apply the supplemental configuration by running a script stored on the *VMware vSphere Configuration Media* disc. To perform this procedure, use a Windows-based device, such as the Network Management (NM) Client, Dispatch Console, or service computer/laptop.

During an upgrade, you must run the script specifically on the newly imported virtual machines if the virtual machines were imported after ESXi was updated.

Prerequisites:

- Obtain the *VMware vSphere Configuration Media* disc.
- Install VMware PowerCLI on the Windows-based device.

Procedure:

1 Into the optical drive of the Windows-based device, insert the *VMware vSphere Configuration Media* disc.

2 Run the PowerShell command prompt as administrator:

   a Click **Start**.

   b In the **Search programs and files** field, enter: `Command Prompt`

   c Right-click **Command Prompt** and select **Run as administrator**.

   If the **User Account Control** window appears, click **Continue** or **Yes**, depending on the prompt you see. If you are not logged on with an administrative account, enter the domain admin credentials.

   d At the command prompt, enter: `powershell`

3 At the PowerShell prompt, enter the drive letter of the optical drive that contains the *VMware vSphere Configuration Media* disc followed by a colon.

   Step example: `E:`

   The directory is changed to the root directory of the *VMware vSphere Configuration Media* disc.

4 At the PowerShell prompt, enter: `cd common\bin`

The directory is changed to the `common\bin` directory of the *VMware vSphere Configuration Media* disc.

5 At the PowerShell prompt, enter: `.\Configure-VMHardening.ps1`

6 At the ESXi host IP prompt, enter the IP address of the ESXi host.

7 At the user name prompt, enter the ESXi host user name for an administrative account.

8 At the password prompt, enter the ESXi host password for an administrative account.

9 At the PowerShell prompt, perform one of the following actions:

- To apply supplemental configuration to all virtual machines on the ESXi host, enter: `All`
- To apply supplemental configuration to a single virtual machine, enter the name of the particular virtual machine.

NOTICE: Ensure that the name matches the name of the virtual machine as it appears in the left pane of the vSphere Client inventory view when connected to the ESXi host.

The virtual machines supplemental configuration is applied.

10 Verify that there are no messages stating `[FAILED]` in the output of the script.

11 At the PowerShell prompt, enter: `exit`

12 At the Windows command prompt, enter: `exit`

This page intentionally left blank.

Chapter 3

Mobile VPN Gateway Configuration

This chapter details configuration procedures relating to an ESXi-based Virtual Server.

3.1 Configuring Virtual Machine Security Settings

When and where to use: Perform this procedure for every Motorola Solutions Mobile VPN Gateway virtual machine.

Procedure:

1. Launch the VMware vSphere Client from the Windows-based device (local machine) on which it resides. You can use **Start** → **Programs** or a desktop shortcut.

   At initial installation, a desktop shortcut was automatically created.

   A dialog box appears prompting for an IP address, user name, and password.

2. Perform the following actions:
   - **a** Type the IP address of the ESXi server.
   - **b** Type the user name `root`
   - **c** Type the root user password of the ESXi server.
   - **d** Click **Login**.

   In redundant configuration, log on to the redundant ESXi server.

   The vSphere **Client Inventory** window appears.

3. Power off the Virtual Machine. If already powered off, skip this step.
   - **a** In the navigation pane, right-click the virtual machine you want to power off.
   - **b** From the **Power** menu, select **Shut Down Guest**.
   - **c** Confirm the shutdown by clicking **Yes**.
4. In the navigation pane, right-click the virtual machine you want to configure.
5. In the pop-up menu, select **Edit Settings**.
6. In the **Edit Settings** dialog box, select the **Options** tab.
7. Under the **Advanced** heading, select **General**.
8. Select **Configuration Parameters**.
9. Add Configuration Variables:
   - **a** Click **Add Row**.
   - **b** In the new row, in the **Name** field, type `isolation.device.connectable.disable`
   - **c** Press TAB and in the **Value** field, type `true`
   - **d** Click **Add Row**.
   - **e** In the new row, in the **Name** field, type `isolation.tools.diskShrink.disable`
   - **f** Press TAB and in the **Value** field, type `true`

g Click **Add Row**.

h In the new row, in the **Name** field, type `isolation.tools.diskWiper.disable`

i Press TAB and in the **Value** field, type `true`

10 Click **OK** on each of the configuration windows that are open.

3.2 Configuring Virtual Machine Resource Settings

When and where to use: Perform this procedure for every Mobile VPN Gateway virtual machine.

Procedure:

1 Launch the VMware vSphere Client from the Windows-based device (local machine) on which it resides. You can use **Start** → **Programs** or a desktop shortcut.

At initial installation, a desktop shortcut was automatically created.

A dialog box appears prompting for an IP address, user name, and password.

2 Perform the following actions:

a Type the IP address of the ESXi server.

b Type the user name `root`

c Type the root user password of the ESXi server.

d Click **Login**.

In redundant configuration, log on to the redundant ESXi server.

The vSphere **Client Inventory** window appears.

3 Power off the Virtual Machine. If already powered off, skip this step.

a In the navigation pane, right-click the virtual machine you want to power off.

b From the **Power** menu, select **Shut Down Guest**.

c Confirm the shutdown by clicking **Yes**.

4 In the navigation pane, right-click the virtual machine you want to configure.

5 In the pop-up menu, select **Edit Settings**.

6 In the **Edit Settings** dialog box, select the **Resources** tab.

7 Select **CPU**.

8 In the text box next to the **Reservation** slider bar, type: `4986`

9 Select **Memory**.

10 Click the checkbox for **Reserve all guest memory (All locked)**.

11 Select **Advanced CPU**.

12 In the **Scheduling Affinity** textbox, type the CPU Affinity values from Table 10: Application, CPU Affinity, and NUMA Parameter on page 62 .

Table 10: Application, CPU Affinity, and NUMA Parameter

Application	CPU Affinity	NUMA
vpngw1	0–3	0

Table continued…

Application	CPU Affinity	NUMA
vpngw2	0–3	0
vpngw3	4–7	0
vpngw4	4–7	0
vpngw5	24–27	1
vpngw6	24–27	1
vpngw7	28–31	1
vpngw8	28–31	1

13 In **Edit Settings**, select the **Resources** tab.

a Select **Advanced Memory**.

b Select the **Use memory from nodes** option.

c Select check box with NUMA value from Table 10: Application, CPU Affinity, and NUMA Parameter on page 62 , specified per application (0 or 1).

14 Click **OK** on each of the configuration windows which are open.

3.3 Configuring the Mobile VPN Gateway General Parameters

It is necessary to configure the Motorola Solutions Mobile VPN Gateway, after import of OVF into the virtual server is completed.

3.3.1 Reconfiguring VMware Tools on Linux-Based Virtual Machine

Procedure:

1 Launch the **VMware vSphere Client** from the Windows-based device where it resides.

A desktop shortcut was created during installation.

2 Log on to the server as `root`.

3 Perform the following actions:

a In the navigation pane of the main window, right-click a Linux-based virtual machine.

b From the menu, select **Power On**.

4 To ensure that the physical CD/DVD drives on the ESXi server are not connected to this guest virtual machine, perform the following actions for each CD/DVD drive:

a In the navigation pane of the main window, right-click the ***<Virtual Machine>*** connected to the DVD drive.

b On the pop-up menu, click **Edit Settings**.

The **Settings** dialog box appears.

c At the **Settings** window, select **Hardware** → **CD/DVD Drive**.

Properties for the **CD/DVD Drive** appear on the right.

d Clear both of the following check boxes if they are available for editing:

- **Connected at power-on**

- **Connected**

  The **Connected** option is available for editing only if the virtual machine is powered on.

e Click **OK**.

5 Perform the following actions:

a In the navigation pane of the main window, right-click the ***<Virtual Machine>***.

b Select **Guest** → **Install/Upgrade VMware Tools**.

The **Install/Upgrade Tools** dialog box appears.

6 Select **Interactive Tools Upgrade** → **OK**.

A virtual CD-ROM containing the VMware tools software is now connected to this virtual machine.

7 Click the **Console** tab for this virtual machine.

8 Log on to the virtual machine as `root`.

9 Enter: `ls -al /etc/.samhain.enabled`

- If the `.samhain.enabled` file does not exist, go to step 10.
- If the `.samhain.enabled` file exists, in the `Console` for the selected Linux Virtual Machine, enter: `/etc/init.d/samhain stop`

The `/etc/init.d/samhain stop` command returns success if the samhain service is enabled, or failure if the samhain service is not enabled. Whichever the result is, go to step 10.

10 Enter: `cp /media/cdrom0/VMwareTools-x.x.x-xxxxxx.tar.gz /tmp/`

If the VMware tool is mounted to `/media/cdrom1` instead to `/media/cdrom0`, in the previous command, enter: `/media/cdrom1`

The ***<x.x.x-xxxxxx>*** variable identifies the version of the tools application installed.

You can use the TAB to auto complete the ***<x.x.x-xxxxxx>***.

To find ***<x.x.x-xxxxxx>***, enter: `ls /media/cdrom0/`

11 Enter: `gunzip /tmp/VMwareTools-x.x.x-xxxxxx.tar.gz`

The variable ***<x.x.x-xxxxxx>***, identifies the version of the tools application installed.

To auto complete the ***<x.x.x-xxxxxx>***, you can use the TAB key.

To find ***<x.x.x-xxxxxx>***, enter: `ls /tmp`

12 Enter: `cd /tmp`

13 Enter: `tar -xvf VMwareTools-x.x.x-xxxxxx.tar`

The ***<x.x.x-xxxxxx>*** variable identifies the version of the tools application installed.

To auto complete the ***<x.x.x-xxxxxx>***, you can use the TAB.

To find ***<x.x.x-xxxxxx>***, enter: `ls /tmp`

List of files being extracted is shown and the command prompt appears.

14 Enter: `cd vmware-tools-distrib`

The command prompt appears.

15 To configure the tools application, as a single line at the prompt enter:

`./vmware-install.pl -default`

`--clobber-kernel-modules=vmxnet3,pvscsi,vmmemctl`

The VMware tools installation completes.

16 Optional: If a prompt appears, perform the following actions:

a Enter: `yes`

b For any other prompts to keep the default values, continue to press ENTER.

17 Unmount the drive, see Unmounting a Drive in vSphere Client on page 113.

18 Right-click the VM name in the left pane of vSphere client. Select **Guest** → **End VMWare tools install**.

19 Enter: `ls -al /etc/.samhain.enabled`

- If the `.samhain.enabled` file does not exist, go to step 20.
- If the `.samhain.enabled` file exists, enter: `/opt/Motorola/clc/sbin/init_samhain_db`

20 Enter: `reboot`

The Virtual Machine reboots.

3.3.2
Configuring the Network Identity

When and where to use: Perform this procedure for every Motorola Solutions Mobile VPN Gateway virtual machine.

Procedure:

1 Launch the **VMware vSphere Client** from the Windows-based device where it resides.

A desktop shortcut was created during installation.

2 Log on to the server as `root`.

3 Perform the following actions:

a In the navigation pane of the **VMware vSphere Client** main window, right-click a Linux-based virtual machine.

b Click the **Console** tab for this virtual machine.

4 In the **Console** window, log on as the `root` user.

5 At the command prompt, enter: `admin_menu`

6 At the **Main Menu**, enter the number associated with **OS Administration**.

7 At the **OS Administration** menu, enter the number associated with **Manage Platform Configuration**.

8 At the **Manage Platform Configuration** menu, enter the number associated with **Set Identity**.

9 Enter ***<Application ID>***.

In a redundant configuration, use consecutive positive integers.

Step example: 2 node cluster has Application IDs `1` and `2`
Step example: 2 node non-redundant cluster has Application IDs `1` and `3`

10 Enter the hostname prefix (up to 9 characters).

You can skip this step by pressing ENTER.

NOTICE:
The hostname prefix must be identical on all nodes.

Hostname must be the same as the name of the Virtual Machine specified upon import of the OVF file to the ESXi server. See Importing OVF into Virtual Server on page 55.

11 If the Mobile VPN Gateway is supported by a DNS server, enter the DNS domain name.

You can skip this step by pressing ENTER.

12 If the Mobile VPN Gateway is supported by a DNS server, enter the DNS server IP address. Separate each IP address with a colon (":").

You can skip this step by pressing ENTER.

13 If the Mobile VPN Gateway is supported by an NTP server, enter the NTP server IP address. Separate each IP address with a colon (":").

You can skip this step by pressing ENTER.

14 If the Mobile VPN Gateway is supported by the Operations Support Platform Backup Manager, enter the UIS server IP address accessible via management (eth0) interface. You can skip this step by pressing **ENTER**.

In order to integrate MVPN Gateway with Enhanced Software Upgrade (ESU) feature, the UIS IP address parameter must be configured on vpngw server with Application ID 1.

NOTICE: In PS-LTE deployment using Geo-Redundancy with `A.B.x.x` as OSP network, MVPN Gateway should be configured with UIS HA virtual address `A.B.15.53`. If Geo-Redundant HA UIS feature is not present, IP address for UIS is `A.B.9.43`.

15 Enter the IP address of the agency network where the Mobile VPN Gateway resides: ***<xxx>.<yyy>.<zzz>.***`0/22`

where:

<xxx> and ***<yyy>*** are the first two octets of the network address

<zzz> is the upper six bits of the 3rd octet

NOTICE: This entry is in the CIDR (IPv4) format. For an example, see step 18.

16 Enter ***<MVPN Cluster ID>***.

For non-geo-redundant configuration using only one MVPN cluster use default value 1.

B. For geo-redundant configuration with multiple MVPN clusters, provide value unique for each MVPN cluster.

Step example: Geo-redundant configuration:

- assign value 1 to MVPN Cluster ID in Geo-Site A
- assign value 2 to MVPN Cluster ID in Geo-Site B

17 At the `Customize Management Network?(y/n)` prompt, perform one of the following actions:

NOTICE: If customized management network is selected, it is required in further steps to always use Customization of IP during the cluster definition process.

If…	Then…
If you want to configure the network automatically,	enter `N` and continue to step 19.
If you want to configure the network manually,	perform the following actions:

If…	Then…
	a Enter `Y` **b** Enter the Management IP address. **c** Enter the Network Gateway IP address. **d** Enter the Network Subnet Mask IP address. **e** Enter `N` and continue to step 18.

18 Optional: Enter Management Network Interface Custom Route(s).

Enter the IP addresses in the CIDR (IPv4) format. Separate each IP address with a colon (":"). See the *System IP Plan*.

NOTICE: If MVPN Gateway is intended to be integrated with OSP features, then UEM, Genesys, and ESU, the OSP subnet (`A.B.0.0/16`) must be added to management network routing list.

NOTICE:
The CIDR (Classless Inter-Domain Routing) is a compact, prefix-based representation for IP addresses and routing properties. It is typically used to represent the IP address and the subnet mask.

Example:
For the CIDR entry: `192.162.101.0/24`, this is interpreted as:

IP: `192.162.101.0`

Subnet mask: `255.255.255.0`

The number after the "/" character, correlates to the subnet mask as:

- `x.x.x.x/8 = 255.0.0.0`
- `x.x.x.x/16 = 255.255.0.0`
- `x.x.x.x/24 = 255.255.255.0`
- `x.x.x.x/32 = 255.255.255.255`

19 Optional: Enter the Centralized Syslog server IP address or hostname. Separate each IP address with a colon (":"). Refer to your customer-specific IP planner. See the note in the previous step, if needed.

You can skip this step by pressing ENTER.

The summary of your settings displays.

20 To confirm the settings, enter: `Y`

The system reboots.

3.3.3
Joining the Mobile VPN Gateway to an Existing Domain Controller

This is an optional procedure. During the Set Identity operation, the user enters the DNS Domain name. The DNS Domain name cannot be changed after the Set Identity operation.

IMPORTANT: Results of this procedure are **not** part of the MVPN backup. If the MVPN system is restored from backup, this procedure must be performed again *after* the restore.

Prerequisites: Ensure application time is within 5 minutes of that of the domain controller. See System Time on the Mobile VPN Gateway on page 68.

When and where to use: Perform this procedure for every Motorola Solutions Mobile VPN Gateway virtual machine only in a system with a centralized logging server.

Procedure:

1. Log on to the server through the vSphere client.
2. At the command line prompt, enter `admin_menu`.
3. At the `Main Menu`, enter the number corresponding to `Services Administration`.
4. At the `Services Administration Menu`, enter the number corresponding to `Manage DNS Client Configuration`.
5. If the DNS Servers have not been set, enter the number corresponding to `Set DNS Server(s)`. Otherwise, skip to step 8.
6. Enter the colon-delimited list of DNS servers. Separate each IP address with a colon (":").
7. At the confirmation prompt, enter `Y`
8. Enter `B`
9. Enter the number corresponding to `Manage AAA Client Configuration`
10. Enter the number corresponding to `Join Domain`
11. At the Domain OU prompt, enter the Domain OU.
12. At the NetBIOS Name prompt, enter the NetBIOS Name.
13. Enter the comma-delimited list of Device Login Groups (if any exist).
14. At the confirmation prompt, enter `Y`
15. At the list of AD Domains, select the menu option for the AD Domain you are attempting to join.
16. At the prompt for Domain Account, enter the user name of the domain administrator.
17. At the prompt for the password, enter the domain administrator password
18. To exit the administration menu, type `Q`

3.3.4
System Time on the Mobile VPN Gateway

Perform the following procedures to configure the Network Time Protocol (NTP) server. A proper NTP setup allows local time synchronization.

3.3.4.1
Adding Remote NTP Source on the Mobile VPN Gateway

Follow this procedure to add a remote NTP Source on the Mobile VPN Gateway. Unavailability of an NTP time source may cause some security certificates be revoked.

When and where to use: Perform this procedure when there are no local NTP time sources available for the Mobile VPN Gateway.

Procedure:

1. Log on to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Services Administration**.

4 At the **Services Administration** menu, enter the number associated with **Manage NTP Client Configuration**.

5 At the **Manage NTP Client Configuration** menu, enter the number associated with **Add External NTP Time Source**.

6 At the prompt, enter the ***<IP address of the NTP server>***.

Each ***<IP address of the NTP server>*** should be added separately.

The following message appears: ***<a.b.c.d>*** `added external NTP time source`, where ***<a.b.c.d>*** is the remote NTP time source IP address.

A remote NTP time source is added.

3.3.4.2
Removing External NTP Time Source on the Mobile VPN Gateway

Follow this procedure to remove a remote NTP Source on the Mobile VPN Gateway. Unavailability of an NTP time source may cause some security certificates be revoked.

When and where to use: Perform this procedure when there is a local NTP time source available and you want to remove a remote NTP time source.

Procedure:

1 Log on to the Mobile VPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `admin_menu`

3 At the **Main Menu**, enter the number associated with **Services Administration**.

4 At the **Services Administration** menu, enter the number associated with **Manage NTP Client Configuration**.

5 At the **Manage NTP Client Configuration** menu, enter the number associated with **Remove External NTP Time Source**.

6 At the prompt, enter the ***<IP address of the NTP server>***.

Each ***<IP address of the NTP server>*** should be added separately.

The following message appears: ***<a.b.c.d>*** `added external NTP time source`, where ***<a.b.c.d>*** is the remote NTP time source IP address.

A remote NTP time source is removed.

3.3.4.3
Displaying NTP Status on the Mobile VPN Gateway

Follow this procedure to display NTP status on the Mobile VPN Gateway.

Procedure:

1 Log on to the Mobile VPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `admin_menu`

3 At the **Main Menu**, enter the number associated with **Services Administration**.

4 At the **Services Administration** menu, enter the number associated with **Manage NTP Client Configuration**.

5 At the **Manage NTP Client Configuration** menu, enter the number associated with **Display NTP Status**.

6 At the prompt, enter the ***<IP address of the NTP server>***.

Each ***<IP address of the NTP server>*** should be added separately.

The following message appears: ***<a.b.c.d>*** `added external NTP time source`, where ***<a.b.c.d>*** is the remote NTP time source IP address.

NTP status is displayed.

3.3.5
Managing Centralized Syslog Client Configuration

When and where to use: Perform this procedure for every Motorola Solutions Mobile VPN Gateway virtual machine only in a system with a centralized logging server.

Procedure:

1 Log in to the Mobile VPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `admin_menu`

3 At the **Main Menu**, enter the number associated with **Service Administration**.

4 At the **Service Administration** menu, enter the number associated with **Manage Syslog Client Configuration**.

5 Enter the number associated with the operation you want to perform:

```
Manage Syslog Client Configuration
**************************************
  1. Add Centralized Logging Server
  2. Remove Centralized Logging Server
  3. Display Centralized Logging Status
  b. Back to Previous Menu
  q. Quit
Enter selection (1-3,b,q):
```

The selected action is performed.

3.3.6
Licensing Administration

MVPN Gateway licensing administration is typically used to increase or decrease user capacity on the MVPN Gateway. It is important to use a license with a capacity that is sized to the number of users (clients) communicating during day-to-day and during peak capacity. This scenario is not a relationship to the maximum number of users. The maximum number supported on the MVPN is 1250 users (clients) per service group, with 5000 total users (clients) total in a system with 4 service groups. From an agency perspective, the maximum number supported is typically much higher than what is required for day-to-day operations and peak usage at the agency. The MVPN Gateway is sized for the agency, and may never need to use the maximum number of users.

NOTICE: Clients using Remote Access profile establish individual VPN tunnels, which counts as individual use of license permissions when connected. Multiple VPN clients using a single Site To Site Profile count as a single use of license permissions.

The MVPN Gateway allows a margin of 5% additional client sessions (IKE sessions) compared to the licenses installed. This margin is needed since the MVPN Gateway may have client sessions that are greater in number than the actual active clients, and for peak usage conditions.

Available client licenses are configured with and without MOBIKE enabled. The license types are:

- Basic License - VPN only, in increments of client capacity, without Mobility (MOBIKE with application steering) enabled.
- Advanced License - VPN, in increments of client capacity, with Mobility (MOBIKE with application steering) enabled.

NOTICE: With the Basic license installed, client connection attempts to use “mobility” are ignored, and any associated VPN connection is dropped.

The MVPN Gateway limits the IKE sessions based on the total number of client license capacities. For example, if there are 50 licenses installed on an MVPN Gateway instance, the MVPN Gateway limits the IKE sessions to 50 (53 with 5% extra margin) for the gateway.

Consult with your Motorola Solutions service representative for capacity sizing for your installation. The capacity sizing may include typical operation and future expansion. For future expansion, projections of client usage for both day-to-day operations and peak usage must be considered.

Obtaining a License

For instructions for obtaining a license, see Obtaining Mobile VPN Gateway UUID for Licensing on page 188 and Retrieving License File from Motorola Licensing Server on page 188.

If needed, contact your Motorola Solutions service representative to discuss the technical aspects of the solution and the required compatible license.

Required information for each client capacity license:

- MVPN UUID
- Client capacity.
- If MOBIKE is enabled or not.

CAUTION: Use care when ordering and installing a new client license file. New license files overwrite the existing license file on the MVPN. It is possible to overwrite a large capacity client license file with a new, smaller capacity file. This situation may not be desired.

3.4 Configure the Mobile VPN Gateway Network

The following is the list of procedures for configuring the hardware for the Public Safety LTE Mobile Virtual Private Network Gateway system.

3.4.1 Manage the VPN Cluster

The following is the list of procedures for configuring the VPN clusters for the Public Safety LTE Mobile Virtual Private Network Gateway system.

3.4.1.1 Accessing the Manage Cluster Configuration Menu

Prerequisites: MVPN Gateway is functioning.

When and where to use:

IMPORTANT: A cluster can only be defined once. (See the caution note in Defining the Cluster on page 72.) Each Virtual Machine is added to the cluster. A typical configuration is four pairs of primary and secondary Virtual Machines, for a total of eight virtual machines. In addition, a service group can be added to the cluster, **after** the cluster is defined.

Procedure:

1. Log in to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **Manage Cluster Configuration**.

Postrequisites: Continue with Manage the VPN Cluster on page 71, Manage the VPN Cluster on page 71, and Displaying Live Statistics on page 130, as needed.

3.4.1.2
Defining the Cluster

This procedure shows an example of defining a redundant cluster.

Prerequisites: Perform Accessing the Manage Cluster Configuration Menu on page 71.

When and where to use:
Create the cluster configuration.

It is recommended to perform this procedure on Motorola Solutions Mobile VPN Gateway 1 (`vpngw1`).

CAUTION: This procedure can be run only once per system installation sequence. If the cluster is not configured correctly, the system installation sequence from Installing and Configuring the Mobile VPN Gateway Servers on page 39 is restarted, starting from OVF import.

NOTICE: IP addresses and other values in the script output shown are examples only. Refer to your customer-specific IP planner.

Procedure:

1. At the **Manage Cluster Configuration** menu, enter the number associated with **Define Cluster**.
2. An interactive script runs. Answer the prompts. Default values are in square brackets “[ ]”.
   - For redundant cluster, enter: `R`
   - For non-redundant cluster, enter: `N`

```
Create VPN Cluster
**********************************************************************
Enter Cluster Name: testLicense
Redundant or Non-redundant?(R or N): R
Enter number IPsec service IPs [1]:
Enter HA Heartbeat timeout (non-zero seconds) [300]:
Enter VMS1 Fence Address(IP): 192.161.0.144
Enter VMS2 Fence Address(IP): 192.161.0.146
Enter Fencing password:
Re-enter Fencing password:

Fencing configuration verification...success
```

3 Optional: Enter the Internal Network Custom Routes in the CIDR (IPv4) format. Separate each IP address with a colon (":"). See the note at step 18 in Configuring the Network Identity on page 65 if needed. Entered values are displayed.

```
Enter Internal Network Custom Route(s)
(optional, colon separated CIDR) []:192.162.3.0/24:192.160.3.0/24

Entered Data for VPN Cluster
**********************************************************************
Cluster Name : testLicense
Redundant or Non-redundant? : R
Number of service groups : 1
HA Heartbeat timeout : 300
Internal Network Custom Route(s) : 192.162.3.0/24:192.160.3.0/24

**********************************************************************
**
VPN    |      Internal          |       External         |          HA
1      | 192.162.1.133/29       | 192.162.2.133/29       |
192.162.1.225/29
2      | 192.162.1.133/29       | 192.162.2.133/29       |
192.162.1.226/29
```

4 Confirm the displayed entries.

NOTICE:
If custom management IP addresses were selected for any of the MVPN Gateway servers, user must use the Customize option by typing `customize` instead of `Y`.

```
Are all entries correct?(y/n/customize): y

Synchronizing.
Creating Service Group.
Node n162-vpngwha1 added.
Node n162-vpngwha2 added.
Method vpn-vms1-fm added to n162-vpngwha1.
Method vpn-vms2-fm added to n162-vpngwha2.
Deploying node 1
Deploying node 2
Done deploying Service Group
Synchronizing cfg files...
```

5 **NOTICE:** Configuration from machine with application ID 1 (vpngw1) will be copied to other machines.

Enter the clusync password. Re-enter the clusync password for verification.

The settings for specific nodes and other details configure automatically.

```
Setting password for the cluster
Changing password for user clusync.
New Password:
Retype new password:

Cluster successfully deployed
```

3.4.1.3

Synchronizing the Cluster Definition

Perform this procedure to synchronize the cluster after updating it. This option typically should not be used. It is needed only when some synchronization problems occurred earlier (node down or connectivity problem).

Prerequisites:
Perform Accessing the Manage Cluster Configuration Menu on page 71.

A defined cluster exists. Perform Defining the Cluster on page 72, if needed.

When and where to use:

NOTICE: IP addresses and other values in the script output shown are examples only. Refer to your customer-specific *System IP Plan*.

Procedure:

At the **Manage Cluster Configuration** menu, enter the number associated with **Synchronize Cluster Definition**.

A synchronization progress message similar to the following displays:

```
Synchronizing.
Creating Service Group.
Node n162-vpngwha1 added.
Node n162-vpngwha2 added.
Method vpn-vms1-fm added to n162-vpngwha1.
Method vpn-vms2-fm added to n162-vpngwha2.
Deploying node 1
Deploying node 2
Done deploying Service Group
Synchronizing cfg files...
```

3.4.1.4

Displaying the Cluster and Status

Prerequisites:
Perform Accessing the Manage Cluster Configuration Menu on page 71.

A defined cluster exists. Perform Defining the Cluster on page 72 if needed.

NOTICE: IP addresses and other values in the script output shown are examples only. Refer to your customer-specific *System IP Plan*.

Procedure:

At the **Manage Cluster Configuration** menu, enter the number associated with **Synchronize Cluster Definition**.

The clusters and status similar to the following is displayed:

```
 SG | Service IP      | Node 1           | Node 2
*********************************************************
 1  | 192.162.2.133   | ONLINE ACTIVE    | ONLINE STANDBY

Note: States marked with a '*' have a clusync user password failure
```

3.4.1.5
Adding a Service Group to the Cluster

Prerequisites:
Perform Accessing the Manage Cluster Configuration Menu on page 71.

A defined cluster exists. Perform Defining the Cluster on page 72 if needed.

NOTICE: IP addresses and other values in the script output shown are examples only. Refer to your customer-specific *System IP Plan*.

When and where to use: Perform this procedure on the Motorola Solutions Mobile VPN Gateway 1 (`vpngw1`).

Procedure:

1. At the **Manage Cluster Configuration** menu, enter the number associated with **Add Service Group to Cluster**.
2. At the interactive script prompt, answer the prompts.

   Default values are in square brackets “[ ]”.

```
Add Service Groups to VPN Cluster
*********************************************************************
Maximum number of new IPsec service IPs is 3.
Enter number new IPsec service IPs to add [1]:

Entered Data for Added Service Groups to VPN Cluster
*********************************************************************
Number of added service groups : 1

*********************************************************************
**
VPN   |      Internal         |       External        |         HA
3     | 192.162.1.141/29      | 192.162.2.141/29      |
192.162.1.227/29
4     | 192.162.1.141/29      | 192.162.2.141/29      |
192.162.1.228/29
Are all entries correct?(y/n/customize): y
Synchronizing.
Creating Service Group.
Node 162-vpngwha3 added.
Node 162-vpngwha4 added.
Method vpn-vms1-fm added to 162-vpngwha3.
Method vpn-vms2-fm added to 162-vpngwha4.
Deploying node 1
Deploying node 2
Synchronizing cfg files...
```

3.4.1.6
Changing the HA Heartbeat Timeout

Prerequisites:
Perform Accessing the Manage Cluster Configuration Menu on page 71.

A defined redundant cluster exists. Perform Defining the Cluster on page 72 if needed.

NOTICE: IP addresses and other values in the script output shown are examples only. Refer to your customer-specific *System IP Plan*.

Procedure:

1. At the **Manage Cluster Configuration** menu, enter the number associated with **Change HA Heartbeat Timeout**.
2. At the interactive script, answer the prompts.

   Default values are in square brackets “[ ]”.

```
Change HA Heartbeat Timeout for VPN Cluster
**********************************************************************
Enter HA Heartbeat timeout(non-zero seconds) [300]: 400
Synchronizing.
Creating Service Group.
Node 162-vpngwha1 added.
Node 162-vpngwha2 added.
Method vpn-vms1-fm added to 162-vpngwha1.
Method vpn-vms2-fm added to 162-vpngwha2.
Deploying node 1
Deploying node 2

Creating Service Group.
Node 162-vpngwha3 added.
Node 162-vpngwha4 added.
Method vpn-vms1-fm added to 162-vpngwha3.
Method vpn-vms2-fm added to 162-vpngwha4.
Deploying node 1
Deploying node 2
Done deploying Service Group
Synchronizing cfg files...
```

3.4.1.7
Changing the Fencing Password

Prerequisites:
Perform Accessing the Manage Cluster Configuration Menu on page 71.

A defined redundant cluster exists. Perform Defining the Cluster on page 72 if needed.

NOTICE: IP addresses and other values in the script output shown are examples only. Refer to your customer-specific *System IP Plan*.

Procedure:

1. At the **Manage Cluster Configuration** menu, enter the number associated with **Change Fencing Password**.
2. At the interactive script prompt, answer the prompts.

```
Change Fencing Password for VPN Cluster
**********************************************************************
Enter VM's Fencing password:
Re-enter VM's Fencing password:

Testing vms01 fencing credentials...success

Testing vms02 fencing credentials...success
Synchronizing.
Creating Service Group.
Node n162-vpngwha1 added.
Node n162-vpngwha2 added.
```

```
Method vpn-vms1-fm added to n162-vpngwha1.
Method vpn-vms2-fm added to n162-vpngwha2.
Reloading node 1
Reloading node 2
Done deploying Service Group
Synchronizing cfg files...
Cluster Fencing Password Changed
```

3.4.1.8
Accessing the Clusync User Credentials Menu

Perform this procedure to check or verify the cluster SSH connectivity, change the cluster password, or change the local clusync password.

Prerequisites:
Perform Accessing the Manage Cluster Configuration Menu on page 71.

When and where to use:

NOTICE: IP addresses, and other values in the script output shown are examples only. Refer to your customer-specific *System IP Plan*.

Procedure:

At the **Manage Cluster Configuration** menu, enter the number associated with **Change Clusync User Credentials**.

The **Change Clusync User Credentials** menu displays.

```
 Change Clusync User Credentials (* - Option not available)
**************************************
  1. Check ssh connectivity
  2. Set cluster password
  3. Change local clusync account password
  b. Back to Previous Menu
  q. Quit
Enter selection (1-3,b,q):
```

3.4.1.8.1
Checking SSH Connectivity

Perform this procedure to display or verify the SSH connectivity of the clusters.

Prerequisites:

1 Perform Accessing the Manage Cluster Configuration Menu on page 71.

2 Perform Accessing the Clusync User Credentials Menu on page 77.

When and where to use:
A defined cluster exists. Perform Defining the Cluster on page 72, if needed.

Perform this procedure on Motorola Solutions Mobile VPN Gateway 1 (`vpngw1`).

NOTICE: IP addresses and other values in the script output shown are examples only. Refer to your customer-specific *System IP Plan*.

Procedure:

At the **Change Clusync User Credentials** menu, enter the number associated with **Check ssh connectivity**.

The cluster SSH `All nodes reachable` status is displayed.

3.4.1.8.2

Setting the Cluster Password

Perform this procedure to update or change the cluster password.

Prerequisites:

1 Perform Accessing the Manage Cluster Configuration Menu on page 71.

2 Perform Accessing the Clusync User Credentials Menu on page 77.

A defined cluster exists. Perform Defining the Cluster on page 72, if needed.

When and where to use:
Perform this procedure on Motorola Solutions Mobile VPN Gateway 1 (`vpngw1`).

IMPORTANT: This function synchronizes with the redundant VM in a redundant cluster.

Procedure:

1 At the **Change Clusync User Credentials** menu, enter the number associated with **Set cluster password**.

2 At the interactive script prompt, answer the prompts.

```
Setting password for the cluster
Changing password for user clusync.
New Password:
Retype new password:
Successfully updated cluster password
```

3.4.1.8.3

Changing the Local clusync Account Password

This procedure changes the local clusync password at a cluster VM.

Prerequisites:

1 Perform Accessing the Manage Cluster Configuration Menu on page 71.

2 Perform Accessing the Clusync User Credentials Menu on page 77.

A defined cluster exists. Perform Defining the Cluster on page 72, if needed.

When and where to use:

CAUTION: This function **does not** synchronize with the redundant VM in a redundant cluster. This procedure is only used during a restore or if adding a (new) service group to the cluster. See Adding a Service Group to the Cluster on page 75 and the Mobile VPN Gateway Server Disaster Recovery on page 167 chapter.

NOTICE: IP addresses and other values in the script output shown are examples only. Refer to your customer-specific *System IP Plan*.

Procedure:

1 At the **Change Clusync User Credentials** menu, enter the number associated with **Change local clusync account password**.

2 At the interactive script prompt, answer the prompts.

Default values are in square brackets “[ ]”.

Step example:

```
                          ***WARNING***
This operation may cause this node to become unreachable from other
```

```
nodes in the cluster. This operation should only be used bring a node
back into sync with the cluster. This operation only sets the linux
users
password and does not modify the internal configuration.

Continue setting local clusync user password (y/n)[n]: y
Changing password for user clusync.
New Password:
Retype new password:
Changing password for user clusync.
passwd: all authentication tokens updated successfully.
```

3.4.2
Managing Static Routing

When and where to use: Use this procedure to add, remove, or list routes on the Motorola Solutions Mobile VPN Gateway. Perform this procedure on odd-numbered Mobile VPN Gateways.

Procedure:

1. Log in to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **Routing Configuration**.
5. Select one of the following interfaces to manage:
   - **Management Network Interface Route**
   - **VPN Internal Network Interface Route**
6. Perform one of the following actions:

If…	Then…
If you want to add a route,	Perform the following actions: **a** Enter the number associated with **Add Route**. **b** Enter the IP address in the CIDR (IPv4) format. See the note at step 18 in Configuring the Network Identity on page 65, if needed. **c** Repeat for adding multiple routes. Add each route separately (one at a time).
If you want to remove a route,	Perform the following actions: **a** Enter the number associated with **Remove Route**. **b** Select the route to remove.
If you want to list routes,	Enter the number associated with **List Routes**. The list displays as a live update. Press `Q` to quit and return to the **Application Administration** menu.

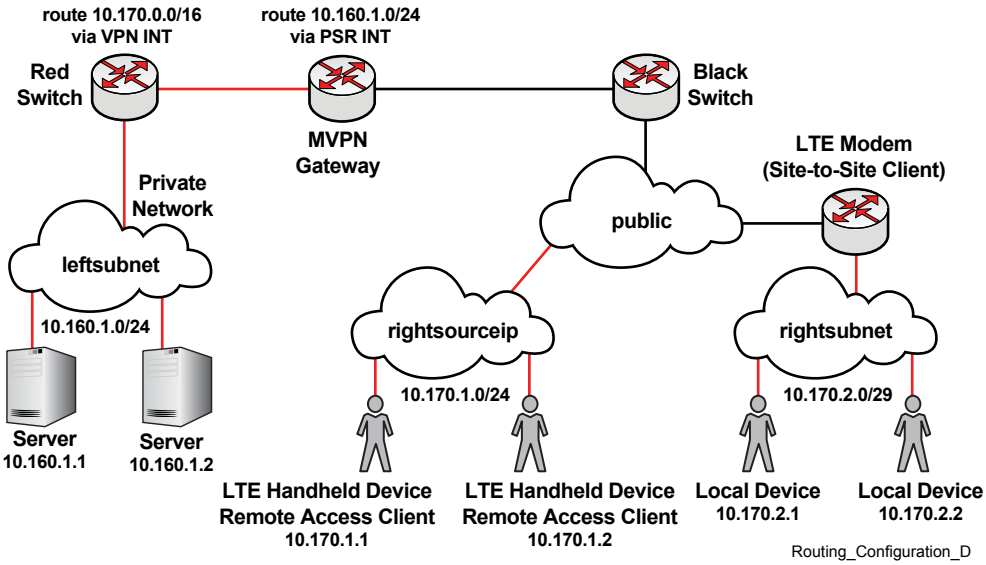
The selected action is performed.

3.4.2.1

Mobile VPN Routing Configuration

The following figure shows an example of the relation between the general network parameters of connection profiles, routing and the Mobile VPN topology.

Figure 12: Mobile VPN Routing Configuration



The **rightsourceip** parameter is part of Remote Access profile configuration.

The **rightsubnet** parameter is part of Site-To-Site profile configuration.

When multiple LTE router devices are used, each device should be configured with an individual local network. The rightsubnet CIDR value should implicitly contain a local router network for each router device.

In Mobile VPN Topology on page 105, Site-to-Site profile is configured with 10.170.2.0/24 rightsubnet value. This rightsubnet value contains 10.170.2.0/29 network assigned to LTE router device.

3.4.2.2

Configuring Management Network Routing for OSP Services, System Restore and Remote Access

When and where to use:
With default settings, only destinations in management subnet A.B.C.0/25 (where C has first 2 bits zeroed) are routed via **eth0** interface.

Services located in OSP domain such as UIS (ESU), Fault Management (UEM), Availability Reports and Performance Management require adding OSP destination in Management Network Interface Route list.

User device from which administrator accesses remotely MVPN GW server with ssh/sftp/scp programs or performs restore operation requires adding device network in Management Network Interface Route list.

To add a route for Management Network Interface, see Managing Static Routing on page 79 procedure.

3.4.2.3
Configuring VPN Internal Routing

By default, no internal destinations are configured for decrypted IPSEC traffic. These destinations need to be added after MVPN cluster has been configured. The destinations which have to be added to VPN Internal Network Interface Route are:

- By default, no internal destinations are configured for decrypted IPSEC traffic. These destinations need to be added after MVPN cluster has been configured.

NOTICE: By default, all inbound OSPF routes are added to VPN Internal Routing. To change this behavior, refer to OSPF Routing Issues on page 148.

The destinations which have to be added to VPN Internal Network Interface Route are:

NOTICE: There is no distinction of treating destinations coming from OSPF and non-OSPF profiles. All of them should be configured.

To add a route for Management Network Interface, see Managing Static Routing on page 79 procedure.

3.4.2.4
Default Routing and Firewall

Before MVPN cluster is configured, the system default routing is set to **eth0** (VPN MGMT) interface. In addition, only type of traffic which can pass through this interface must listed in internal firewall settings. User is not intended to change firewall settings for management interface.

After MVPN cluster is configured, the system default routing is set to **eth2** (VPN EXT) interface. In addition, only type of traffic which can pass through this interface is **IPSEC/E-UDP IPSEC** or port-specific **UDP/TCP** configured with local bypass rules.

3.4.3
Configuring OSPF

Prerequisites: Perform Defining the Cluster on page 72.

When and where to use: Perform this procedure to configure admission to the OSPF area within which the advertisement of OSPF routes of client VPN subnets should happen. This procedure should be performed on each service group. OSPF advertisement works for OSPF-specific connection profiles and requires configured OSPF support on an adjacent router.

NOTICE: This procedure supports OSPF for Public Safety LTE starting at release 11.0.

Procedure:

1. Log in to the Mobile VPN Gateway. See Logging on to the Mobile VPN Gateway on page 111.
2. From the command prompt, enter: `admin_menu`
3. From the **Main Menu**, enter the number associated with **Application Administration**.
4. From the **Application Administration** menu, enter the number associated with **OSPF Configuration**.
5. From the **OSPF Configuration** menu, enter the number associated with action:
   - **Set OSPF Global Parameters**

- **Display OSPF Configuration**

6 Perform one of the following actions:

If...	Then...
If you want to configure OSPF for Mobile VPN Gateway,	Enter the number associated with **Set OSPF Global Parameters**. **a** Select area type: **normal**, **nssa**, or **nssa no-summary**. **b** Provide **area id** value 32-bit integer or value in IP address format. **c** Select **authentication type** mode: **message-digest, plain-text, or null** **d** Enter Dead Interval Timer value (in seconds). This value must be the same for all routers attached to the OSPF area. **e** Enter Hello Interval Timer value (in seconds). This value must be the same for all routers attached to the OSPF area. **f** If the following type of authentication is selected: • **message-digest** or • **plain-text** provide password and repeat. **g** Verify your changes.
If you want to see OSPF configuration,	Enter the number associated with **Display OSPF Configuration**.

Step Example

```
 Application Administration (* - Option not available)
**************************************
  1. Preshared Keys Administration
  2. Certificates Administration
  3. High Availability Administration
  4. Manage Cluster Configuration
  5. IPsec Configuration
  6. Statistics Administration
  7. Radius Server Administration
  8. Routing Configuration
  9. Bypass Configuration
 10. Licensing Administration
 11. OSPF Administration
 12. IPSec Log Settings
 13. Perform Log Analyze
  b. Back to Previous Menu
  q. Quit
Enter selection (1-13,b,q): 11
```

```
 OSPF Administration (* - Option not available)
**************************************
  1. Set OSPF Global Parameters
  2. Display OSPF Configuration
  b. Back to Previous Menu
  q. Quit
```

```
 OSPF Administration (* - Option not available)
**************************************
  1. Set OSPF Global Parameters
  2. Display OSPF Configuration
  b. Back to Previous Menu
  q. Quit
Enter selection (1-2,b,q): 1

  1. normal
  2. nssa
  3. nssa no-summary
Select area type (1-3)[1]:
Enter the area id [0.0.0.0]:
Enter Dead-interval timer (seconds) (1-65535)[40]:
Enter Hello-interval timer (seconds) (1-65535)[10]:

  1. message-digest
  2. null
  3. plain-text
Select authentication type (1-3)[2]: 1
Enter the authentication key :
Re-enter the authentication key:
The following values will be set:
  Area type: normal
  Area id: 0.0.0.0
  Dead-interval timer: 40
  Hello-interval timer: 10
  Authentication type: message-digest
  Authentication key: ********
Are you sure you want to continue (y/n/q) : y
OSPF successfully configured
```

```
OSPF Administration (* - Option not available)
**************************************
  1. Set OSPF Global Parameters
  2. Display OSPF Configuration
  b. Back to Previous Menu
  q. Quit
Enter selection (1-2,b,q): 2
 OSPF Routing Process, Router ID: 192.163.2.133
 Supports only single TOS (TOS0) routes
 This implementation conforms to RFC2328
 RFC1583Compatibility flag is disabled
 OpaqueCapability flag is disabled
 Initial SPF scheduling delay 200 millisec(s)
 Minimum hold time between consecutive SPFs 1000 millisec(s)
 Maximum hold time between consecutive SPFs 10000 millisec(s)
 Hold time multiplier is currently 1
 SPF algorithm last executed 1.985s ago
 SPF timer is inactive
 Refresh timer 10 secs
 This router is an ASBR (injecting external routing information)
 Number of external LSA 0. Checksum Sum 0x00000000
 Number of opaque AS LSA 0. Checksum Sum 0x00000000
 Number of areas attached to this router: 1

 Area ID: 10.0.0.100 (NSSA)
   Shortcutting mode: Default, S-bit consensus: ok
   Number of interfaces in this area: Total: 1, Active: 1
   It is an NSSA configuration.
   Elected NSSA/ABR performs type-7/type-5 LSA translation.
   It is not ABR, therefore not Translator.
   Number of fully adjacent neighbors in this area: 0
```

```
Area has message digest authentication
Number of full virtual adjacencies going through this area: 0
SPF algorithm executed 1 times
Number of LSA 1
Number of router LSA 1. Checksum Sum 0x0000bdd2
Number of network LSA 0. Checksum Sum 0x00000000
Number of summary LSA 0. Checksum Sum 0x00000000
Number of ASBR summary LSA 0. Checksum Sum 0x00000000
Number of NSSA LSA 0. Checksum Sum 0x00000000
Number of opaque link LSA 0. Checksum Sum 0x00000000
Number of opaque area LSA 0. Checksum Sum 0x00000000
```

3.4.4
Bypass Configuration Functions

3.4.4.1
Accessing the Bypass Configuration Menu

Perform this procedure to obtain access to configure or display MVPN bypass functions.

Bypass enables direct access to specific TCP and UDP ports of a device working in a public network from a protected network. For example, some devices in a public network (firewalls, routers) may require additional configuration using SSH. Connections to these devices should be established outside of the VPN tunnel.

Prerequisites: Ensure the MVPN Gateway is functioning.

Procedure:

1. Log in to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **Bypass Configuration**.

   The **Bypass Configuration** menu displays.

3.4.4.2
Adding a Bypass Configuration

Perform this procedure to create a bypass configuration.

Prerequisites: Perform Accessing the Bypass Configuration Menu on page 84.

Procedure:

1. At the **Bypass Configuration** menu, enter the number associated with **Add Bypass Configuration**.
2. Answer the prompts by selecting either `upd` or `tcp` for the new bypass configuration rule. Enter a port number and an IP address in CIDR format at the prompts, and verify the new bypass configuration rule.

   NOTICE: The output screen responses for `upd` or `tcp` are similar.

   Step example:

```
  1. udp
  2. tcp
Select the transport protocol (1-2): 1
Enter the port number : 100
Enter the rule network (CIDR) : 192.162.101.0/24

The following rules are about to be added to the iptables firewall:
  -A FORWARD -i eth2 -s 192.162.101.0/24 -p udp -m udp --sport 100 -m
comment --comment "User Defined" -j ACCEPT
  -A FORWARD -o eth2 -d 192.162.101.0/24 -p udp -m udp --dport 100 -m
comment --comment "User Defined" -j ACCEPT
Do you wish to proceed (y/n/q) : y

Successfully added firewall bypass rules.
```

3.4.4.3
Removing a Bypass Configuration

Perform this procedure to delete the bypass configuration.

Prerequisites: Perform Accessing the Bypass Configuration Menu on page 84.

Procedure:

1. At the **Bypass Configuration** menu, enter the number associated with **Remove Bypass Configuration**.
2. At the output of the current bypass rules display, select the desired rule to remove, and verify the removal. Answer any other prompts related to the rule to remove.

   Step example:

```
  1. -A FORWARD -s 192.162.101.0/24 -i eth2 -p udp -m udp --sport 100 -
m comment --comment "User Defined" -j ACCEPT
  2. -A FORWARD -d 192.162.101.0/24 -o eth2 -p udp -m udp --dport 100 -
m comment --comment "User Defined" -j ACCEPT
Select a rule to remove (1-2): 1

A corresponding rule exists.
Selected rule:
  -A FORWARD -s 192.162.101.0/24 -i eth2 -p udp -m udp --sport 100 -m
comment --comment "User Defined" -j ACCEPT
Corresponding rule:
  -A FORWARD -d 192.162.101.0/24 -o eth2 -p udp -m udp --dport 100 -m
comment --comment "User Defined" -j ACCEPT
Remove corresponding rule as well (y|n) : y

The following rules are about to be removed from the iptables firewall:
  -A FORWARD -s 192.162.101.0/24 -i eth2 -p udp -m udp --sport 100 -m
comment --comment "User Defined" -j ACCEPT
  -A FORWARD -d 192.162.101.0/24 -o eth2 -p udp -m udp --dport 100 -m
comment --comment "User Defined" -j ACCEPT
Do you wish to proceed (y/n/q) : y

Successfully removed firewall bypass rule(s).
```

3.4.4.4
Displaying the Bypass Configuration

Prerequisites: Perform Accessing the Bypass Configuration Menu on page 84.

Procedure:

1. At the **Bypass Configuration** menu, enter the number associated with **Display Bypass Configuration**.
2. An output of the current statistics monitoring displays. The screen is refreshed every 2 seconds until the user presses Q to quit.

   Step example:

```
The currently configured bypass rules are:
  -A FORWARD -s 192.162.101.0/24 -i eth2 -p udp -m udp --sport 100 -m
comment --comment "User Defined" -j ACCEPT
  -A FORWARD -d 192.162.101.0/24 -o eth2 -p udp -m udp --dport 100 -m
comment --comment "User Defined" -j ACCEPT
```

3.4.5
Mobile VPN Gateway MTU

In Mobile VPN Gateway, transport overhead depends on each deployment and it is significant in the overall calculation of the MVPN Gateway maximum transmission unit (MTU). The MTU of user payload is substantially less than the typical 1500 MTU used for ethernet. With LTE, the additional overhead of all the layers of security and transport protocols adds significantly to the overhead of user payload.

There are three layers of packet encapsulation occurring on the WAN interface, with the following corresponding MTUs:

- eNB-EPC MPLS: 8 bytes
- eNB-S/GW GTP: 40 bytes
- eNB-SecGW IPsec: 88 bytes (ESP-AES-CBC, with AH SHA-1 and NAT-T)

The total assumed WAN transport overhead is 136 bytes. The maximum PDU size for the MVPN IPsec packet is 1364 bytes.

MVPN Overhead with Suite-B Ciphers

A user's 1302 MTU packet results in a Suite-B IPsec ESP encapsulated MVPN packet of 1364 octets.

The user's original data packet is then encapsulated within a Suite-B ESP packet, with the overhead assumptions as shown in Table 11: MVPN Overhead with Suite-B Ciphers on page 86.

NOTICE: The standard used here is ESP-GCM-128/192/256 bit cipher, which includes integrity protection.

Table 11: MVPN Overhead with Suite-B Ciphers

Field Name	Octets (length)
New IP Header (Tunnel Mode)	20
UDP Header (NAT-T)	8
SPI (ESP Header)	4
Sequence (ESP Header)	4
ESP-GCM Initialization Vector	8
Original Data Packet	1302 (user's tunneled IP datagram)
ESP-GCM Pad	0

Table continued…

Field Name	Octets (length)
Pad (ESP Trailer)	1
Next Header (ESP Trailer)	1
ESP GCM ICV	16
Total	1364

MVPN Overhead with AES–256–CBC encryption using SHA1 Cipher

A user's 1294 MTU packet results in an AES CBC IPsec ESP encapsulated MVPN packet of 1360 octets.

The user's original data packet is then encapsulated within a Suite-B ESP packet, with the overhead assumptions as shown in Table 12: MVPN Overhead with AES–256–CBC encryption using SHA1 Cipher on page 87.

Table 12: MVPN Overhead with AES–256–CBC encryption using SHA1 Cipher

Field Name	Octets (length)
New IP Header (Tunnel Mode)	20
UDP Header (NAT-T)	8
SPI (ESP Header)	4
Sequence (ESP Header)	4
ESP-AES Initialization Vector	16
Original Data Packet	1294 (user's tunneled IP datagram)
ESP-AES Pad	0
Pad (ESP Trailer)	1
Next Header (ESP Trailer)	1
ESP-SHA ICV	12
Total	1360

3.4.5.1

Modifying Mobile VPN Gateway MTU

Perform this procedure to change the maximum transmission unit (MTU) in the Mobile VPN Gateway.

NOTICE: The default MTU size after installation is 1296.

Procedure:

1. Log in on each server as a root user.
2. To set appropriate MTU values for both "default" and "eth1" parameters, edit the file configuration.
   a. In command prompt, execute the following command: `/etc/opt/Motorola/vpn/admin/config/mtu.cfg`.
   b. For VPN traffic packets, set the "default" MTU size parameter to an appropriate value.
   c. For plain traffic packets, set the "eth1" MTU size parameter to an appropriate value.

3 In command prompt, execute the following command: `/opt/Motorola/vpn/admin/bin/set_mtu`.

The new MTU size is applied to actual network interfaces and boot configuration.

3.5 Device Authentication Method Configuration

The default method of authentication in the Motorola Solutions Mobile VPN Gateway is based on certificate chains. ECDSA and RSA are two supported algorithms. Additionally, the Mobile VPN Gateway supports pre-shared keys as an alternative in systems that include an ASTRO® 25 network or pre-shared key supporting devices.

3.5.1 Certificates Administration

Certificates are used to authenticate connections between computers and/or between servers and clients. The following describes the procedures related to Mobile VPN Gateway certificates included in this manual. Contact your Motorola Solutions service representative, for coordination and transferring certificate requests and the resulting certificate files with a designated, trusted, Certificate Authority.

The default method of authentication in the Motorola Solutions Mobile VPN Gateway relies on Public Key Infrastructure. For details, see Mobile VPN Gateway Encryption Keys and Certificate Requirements on page 32.

To create a proper certificate chain to use on the Mobile VPN Gateway, generate a Certificate Signing Request (CSR). The Generating the Certificate Signing Request on page 88 procedure also results in the public-private keys pair generation. The private key is stored on the MVPN Gateway. Based on the public key, the CSR is generated.

Certificate Signing Requests (CSR) are created (generated) at the Mobile VPN Gateway server. The CSR is transferred using secure media (CD/DVD) to the Certificate Authority (CA). A private or other trusted Certificate Authority, depending on the customer need, is used for the generation of the certificate. The Certificate Authority generates a signed certificate (and associated files, certificate chain) for the server. The signed server certificate (and certificate chain) is then transferred using secure media back to the Mobile VPN Gateway server. The signed certificate (and certificate chain) is installed, and imported on the Mobile VPN Gateway server.

For generating the certificate signing request (CSR) and to install and import, update or remove certificates, continue with the next sections.

NOTICE: The Certificate Chain for MPVN refers to the TA Certificate and the Gateway Certificate with optional CA Certificates between them.

NOTICE: Different certificate chains may be used on each of the eight gateways. However, the certificate chain names within a single redundant pair must match. Certificate chains are generated and installed separately on the primary and secondary gateways of the redundant pair. Certificate chains are not migrated across the redundant (primary/secondary) pair.

3.5.1.1 Generating the Certificate Signing Request

Prerequisites: Perform Manage the VPN Cluster on page 71.

When and where to use: Use this procedure on all Motorola Solutions Mobile VPN Gateway virtual machines and only for systems that require the Mobile VPN Gateway to use certificates from a trusted Certificate Authority. See Certificates Administration on page 88 for more discussion about the CSR.

Procedure:

1. Log in to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.

2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **Certificates Administration**.
5. At the **Certificates Administration** menu, enter the number associated with **Generate Certificate Signing Request**.
6. At the **Generate Certificate Signing Request** menu, enter the desired number from the Certificates Encryptions Algorithms list.
7. Enter the common name.

   The common name has a default value which is the fully qualified hostname of the Mobile VPN Gateway.

8. Enter the organizational unit `0`.

   The default value is provided in square brackets.

9. Enter the organizational unit `1`.

   The default value is provided in square brackets.

   NOTICE: The value entered for organizational unit 1 is used to distinguish certificates used for different connection profiles.

10. Enter the organization name.
11. Optional: Enter the locality.

    To skip this step press ENTER.

12. Optional: Enter the state or province name.

    To skip this step press ENTER.

13. Optional: Enter the country name.

    To find your country name, use the ISO 3166-1 alpha-2 code.

    To skip this step press ENTER.

14. Optional: Enter the subject alternative names (***<SubjectAltName>***) in a comma-separated list (Enter "." for no SAN) `[vpngw1, vpngw1, 192.162.2.133]`

    To skip this step press ENTER.

    NOTICE: The default for the ***<SubjectAltName>*** includes the physical IP address of the MVPN Gateway. If the MVPN Gateway is behind a NAT, the ***<SubjectAltName>*** specified during the creation of the CSR should include the NATed IP address of the MVPN server either in addition to, or instead of the physical IP address.

    The summary of CSR configuration displays.

15. Confirm the settings by entering: `Y`

    The generated CSR file is saved in the user home directory.

16 Copy the CSR to secure media (CD/DVD).

17 Optional: Make another copy of the CSR for disaster recovery purposes. Store the media in a secure location.

Postrequisites: Contact your Motorola Solutions service representative, for coordination and transferring certificate requests and the resulting certificate files with a designated, trusted, Certificate Authority. Transfer the CSR media to the certificate authority to generate and export signed certificates to secure media (CD/DVD) for importing to the Mobile VPN Gateway (see Importing the Certificate Chain on page 90).

3.5.1.2

Importing the Certificate Chain

Use this procedure only for systems that require the Mobile VPN Gateway to use certificates from a trusted Certificate Authority.
See also Certificate Chain Issues on page 140.

Prerequisites: Media (CD/DVD) containing the requested, signed certificates from the certificate authority.

When and where to use: Use this procedure for every Mobile VPN Gateway virtual machine only for systems that require the Mobile VPN Gateway to use certificates from a trusted Certificate Authority.

Procedure:

1 Insert a CD/DVD with the certificate chain into the optical drive of the Windows-based local machine.

2 Mount the drive.

See Mounting a Drive in vSphere Client on page 112.

3 Log in to the Mobile VPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

4 At the command prompt, enter: `admin_menu`

5 At the **Main Menu**, enter the number associated with **Application Administration**.

6 At the **Application Administration** menu, enter the number associated with **Certificates Administration**.

7 At the **Certificates Administration** menu, enter the number associated with **Import Certificate Chain**.

The certificate chains available for import are displayed with a prompt for selection:

```
Pick a Certificate Chain to Import (1):
```

8 Each available certificate in the certificate chain is displayed for selection, with the option to bypass the certificate by pressing `q`. Press ENTER to select the desired certificates.

NOTICE: Only available certificates are displayed.

The available certificates are displayed in sequence:

```
Host Certificate
(q to continue)

TA Certificate
(q to continue)
```

9 At the prompt, enter: `y` or `n` to confirm the import of the certificate chain.

10 Enter a name for the selected certificate chain at the next prompt and press ENTER.

The following prompt is displayed:

```
Enter a nickname for this chain:
<new_name_of_certificate_chain>
```

NOTICE: For redundant clusters, the certificate chain names on primary, and secondary gateways must match.

11 Verify the confirmation message is displayed with the new name of the certificate chain.

The following prompt is displayed:

```
Successfully imported chain: <new_name_of_certificate_chain>
```

12 Unmount the drive.

See Unmounting a Drive in vSphere Client on page 113.

3.5.1.3 Removing the Certificate Chain

When and where to use: Use this procedure for every Motorola Solutions Mobile VPN Gateway virtual machine only for systems that require the Mobile VPN Gateway to use certificates from a trusted Certificate Authority.

Procedure:

1. Log in to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **Certificates Administration**.
5. At the **Certificates Administration** menu, enter the number associated with **Remove Certificate Chain**.

   NOTICE: This procedure also deletes the private key associated with the removed chain. The removed chain cannot be re-imported in the future, and the associated CSR (based on which the original chain was generated) cannot be re-used. See Generating the Certificate Signing Request on page 88 for the procedure to generate a new CSR from a new private key. That new CSR can be used to obtain a new certificate chain from a trusted Certificate Authority. See Certificates Administration on page 88 for more discussion about the CSR.
6. Select the certificate chain to remove. Press Y or N to answer the next prompt.

   A warning and confirmation prompt are displayed.

```
 docsChain
*************************************
  Key Spec: RSA-2048
      Host: CN=n162-vpngw1.sysb.com,OU=IPsec,OU=Public
Safety,O=doc,C=US
        TA: C=XX,L=Default City,O=Default Company Ltd

------------------------------------------------------------
                        WARNING !!!
  This action will delete the chain from the store.  The
private key associated with the chain will also be deleted
```

```
------------------------------------------------------------

Do you wish to permanently delete this chain (y/n)[n]:
```

7 Enter: `y`

The action is confirmed.

```
Chain docsChain successfully removed.
```

3.5.1.4
Displaying the Certificate Chain Information

When and where to use: Use this procedure only for systems that require the Motorola Solutions Mobile VPN Gateway to use certificates from a trusted Certificate Authority.

Procedure:

1 Log in to the Mobile VPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `admin_menu`

3 At the **Main Menu**, enter the number associated with **Application Administration**.

4 At the **Application Administration** menu, enter the number associated with **Certificates Administration**.

5 At the **Certificates Administration** menu, enter the number associated with **Display Certificate Chain Information**.

The list of certificate chains displays.

3.5.1.5
Removing the Certificate Revocation List

When and where to use: Update the Certificate Revocation List (CRL) by removing the existing CRL. See Certificate Revocation List (CRL) on page 33.

Procedure:

1 Log in to the Mobile VPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `admin_menu`

3 At the **Main Menu**, enter the number associated with **Application Administration**.

4 At the **Application Administration** menu, enter the number associated with **Certificates Administration**.

5 At the **Certificates Administration** menu, enter the number associated with **Remove Certificate Revocation List**.

The existing Certificate Revocation List (CRL) is removed. A successful message is displayed.

3.5.2
Pre-Shared Keys Administration

As an alternative to certificates based on public key cryptography, it is possible to use symmetric cryptography using pre-shared keys in an ASTRO®25 system or with pre-shared key supporting devices.

3.5.2.1
Adding Pre-Shared Keys for ASTRO Subscriber

Prerequisites: Perform Manage the VPN Cluster on page 71.

When and where to use: Use this procedure on the active Motorola Solutions Mobile VPN Gateway only for LTE data services for the ASTRO®25 system, and other features using pre-shared keys for ASTRO Subscriber.

Procedure:

1. Log in to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **Preshared Keys Administration**.
5. At the **Preshared Keys Administration** menu, enter the number associated with **Store Key**.
6. Enter the number associated with the **AES256–HEX** key.
7. Enter the pre-shared key identifier (Enter the pre-shared key identifier using the following format: ***<<entity>@<key_description>>***.
8. Enter the pre-shared key string.

   The pre-shared key string must consist of `0x`***< <64 hexadecimal characters>>***.

   NOTICE: The key string and format used must be the same as provided at the Key Variable Loader (KVL).
9. Reenter the pre-shared key string.

   The key is added and saved.

3.5.2.1.1
Pre-Shared Keys Identifier Format for ASTRO Subscriber

ASTRO Subscriber PSK identifier consists of a key phrase (text characters) or a series of hexadecimal characters.

For example:

*@APCO_P25.00.84-1003 (using standard APCO values)

SerialNumber-SUID@APCO_P25.MFID.ALGID-KEYID

Subscriber example:

123ABC1234-091193D4991C5F@APCO_P25.00.84-1003

3.5.2.2
Adding Pre-Shared Keys for ASTRO Site-To-Site

When and where to use: Use this procedure on the active Motorola Solutions Mobile VPN Gateway only for LTE data services for the ASTRO®25 system, and other features to add pre-shared keys for ASTRO Site-To-Site.

Procedure:

1. Log in to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. From the command prompt, enter: `admin_menu`.
3. From the **Main Menu**, enter the number associated with **Application Administration**.
4. From the **Application Administration** menu, enter the number associated with **Preshared Keys Administration**.
5. From the **Preshared Keys Administration** menu, enter the number associated with **Store Key**.
6. Enter the number associated with the **IKE1-PLAIN** key.
7. Enter the **Password Identifier** (textual label for PSK password).

   NOTICE: Password Identifier consists of alphnumeric, dot, and underline characters and between 3 to 20 characters long.
8. Enter the plain password string.

   PSK password length is between 9 to 64 characters. Input value must be surrounded by double quote characters.
9. Reenter the pre-shared key string.
10. Enter IP address (if password applies to single address). The default value is provided in square brackets `[%any]`: When IP address defined, it affects if given PSK value can authenticate client with its external IP.

The key is added and saved.

3.5.2.3
Displaying Pre-Shared Keys for ASTRO Subscribers

When and where to use: Use this procedure only for LTE data services for the ASTRO®25 system and subscribers, and other features using pre-shared keys.

Procedure:

1. Log in to the MVPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **Preshared Keys Administration**.
5. At the **Preshared Keys Administration** menu, enter the number associated with **List Keys**.
6. Enter the number associated with the **AES256-HEX** key.
7. Perform one of the following actions:
   - To list all the Pre-Shared Keys, enter `all`.

- To list the Pre-Shared Keys according to a particular device identifier, enter ***<device_identifier>***.
- To list the Pre-Shared Keys according to a particular key identifier, enter the key identifier.
- To list the Pre-Shared Keys according to a full identifier, enter the full identifier.

The list of pre-shared keys displays.

3.5.2.4
Displaying Pre-Shared Keys for ASTRO Site-to-Site

When and where to use: Use this procedure only for LTE data services for the ASTRO®25 system, and other features using pre-shared keys.
Context for the current task

Procedure:

1. Log in to the MVPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **Preshared Keys Administration**.
5. At the **Preshared Keys Administration** menu, enter the number associated with **List Keys**.
6. Enter the number associated with the **IKE1-PLAIN** key.
7. Perform one of the following actions:
   - To list all the Pre-Shared Keys, enter `all`.
   - To list the Pre-Shared Keys according to a particular password identifier, enter ***<password_identifier>***.
   - To list the Pre-Shared Keys according to a particular scope, enter ***<%any>*** or ***<IP address>***.

   The list of pre-shared keys displays.

3.5.2.5
Deleting Pre-Shared Keys

Use this procedure only for LTE data services for the ASTRO®25 system, and other features using pre-shared keys.

When and where to use: Use this procedure on the active Motorola Solutions Mobile VPN Gateway only for LTE data services for the ASTRO®25 system, and other features using pre-shared keys.

Procedure:

1. Log in to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **Preshared Keys Administration**.

5 At the **Preshared Keys Administration** menu, enter the number associated with **Delete Keys**.
6 Select a pre-shared key type.
7 Enter the full identifier.

The selected key is deleted.

3.5.3
RADIUS Authentication

RADIUS authentication is intended to use on Windows PC equipment and requires Microsoft Windows Active Directory to authenticate VPN clients with username and password.

3.5.3.1
Setting Up MVPN Server to Client Authentication Including Active Directory

Prerequisites:
Install and configure the server. See Installing and Configuring the Mobile VPN Gateway Servers on page 39.

For the procedures in this section, record information entered and store in a secure location.

When and where to use: The process applies to the MVPN server in the PS LTE network.

Process:

1 Perform the Configuration Procedure Overview on page 195 procedure.
2 Ensure that time on both the Active Directory server and the MVPN server are set accurately.

See System Time on the Mobile VPN Gateway on page 68.

3 Perform the Generating the Certificate Signing Request on page 88 procedure.

Transfer the Certificate Signing Request (CSR) to the PKI solution. The PKI solution returns a signed certificate chain. Transfer all certificate files to CD/DVD or secure USB for use in the subsequent procedure.

4 Import the certificate chain on the MVPN server.

See Importing the Certificate Chain on page 90.

5 Perform the Adding a RADIUS Server Configuration on page 98 and Creating a Server Connection Profile on page 100 procedures.
6 Perform the Setting Global Parameters for Connection Profiles on page 109 procedure.
7 Import certificates as part of configuring the VPN clients on user equipment such as handhelds, mobile workstations, and vehicular subscriber modems.

For examples, see Configuring User Equipment for Motorola Solutions VPN Service on page 171.

3.5.3.2
RADIUS Configuration for MVPN Servers

The primary and secondary RADIUS server configurations are established for communication and “pass-through” authentication with the Active Directory server, using username/password authentication.

NOTICE: This configuration and following procedures apply to PS LTE systems.

The RADIUS server configuration, and the associated connection profile, apply to a service group on the MVPN gateways cluster.

For the redundant MVPN gateways cluster configuration (primary and secondary servers) the procedures Adding a RADIUS Server Configuration on page 98 and Creating a Server Connection Profile on page 100, when performed on the primary gateway of a group, automatically propagate to the secondary gateway. Since the configuration and profile are propagated for the redundant pair, the procedures are performed only once for a service group. Perform the following procedures for a service group. If needed, optional steps are given for corrections and modifications.

IMPORTANT: The “shared secret” password created during the Adding a RADIUS Server Configuration on page 98 procedure must match the one created in: “step 4” in Creating the RADIUS Clients and Adding a VPN Gateway Network Policy on page 202.

1 Accessing the RADIUS Server Administration Menu on page 97
2 Adding a RADIUS Server Configuration on page 98
3 Optional: Removing a RADIUS Server Configuration on page 98
4 Optional: Updating a RADIUS Server Configuration on page 99
5 Optional, also used to verify the configuration: Displaying a RADIUS Server Configuration on page 100
6 Creating a Server Connection Profile on page 100
7 Creating Connection Profile for Microsoft Windows Clients Using Active Directory (Radius) Authentication

3.5.3.2.1

Accessing the RADIUS Server Administration Menu

Perform this procedure to navigate to the RADIUS Server Administration Menu from the main administration menu.

Prerequisites:

- The cluster is configured. See Defining the Cluster on page 72
- The certificate chain is imported.. See Importing the Certificate Chain on page 90
- The network Active Directory server is configured.
- The network Domain controller is configured.
- The network RADIUS server is configured. See Creating the RADIUS Clients and Adding a VPN Gateway Network Policy on page 202.

See RADIUS Configuration for MVPN Servers on page 96 for general information about topics in this section.

Procedure:

1 Log in to the Mobile VPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `admin_menu`
3 At the **Main Menu**, enter the number associated with **Application Administration**.
4 At the **Application Administration** menu, enter the number associated with **Radius Server Administration**.

Postrequisites: Continue with Adding a RADIUS Server Configuration on page 98, Creating a Server Connection Profile on page 100, and Creating Connection Profile for Microsoft Windows Clients Using Active Directory (Radius) Authentication to set up the primary and secondary RADIUS configuration and the authentication with the Active Directory server.

3.5.3.2.2
Adding a RADIUS Server Configuration

Prerequisites:
Perform Accessing the RADIUS Server Administration Menu on page 97.

You have obtained the “shared secret” password.

When and where to use: To set up the authentication between the client and the MVPN through the RADIUS server (Active Directory).

Procedure:

1. At the **Radius Server Administration** menu, enter the number associated with **Add Radius Server Configuration**.
2. Select the server at the prompt:

```
Configured Radius Servers
*************************************
  1. Primary
  2. Secondary
  Select the type of radius server to add (1-2):2
```

   NOTICE: Only the existing, configured RADIUS servers are displayed.

3. Enter the IP address or FQDN of the RADIUS Server.
4. Enter the RADIUS “shared secret”.

   See Creating the RADIUS Clients and Adding a VPN Gateway Network Policy on page 202.
5. Enter the number of sockets.

   The default value is provided in square brackets.
6. Verify the values displayed. Enter: `y` to confirm.

```
The following values will be set:
  Server: Secondary
  Address: 192.160.3.1
  Sockets: 100
  Secret: ********
Are you sure you want to continue (y/n/q) : y
Radius server configuration successfully added
```

Postrequisites: Continue with Creating a Server Connection Profile on page 100 and Creating Connection Profile for Microsoft Windows Clients Using Active Directory (Radius) Authentication to set up authentication with the Active Directory server.

3.5.3.2.3
Removing a RADIUS Server Configuration

Prerequisites: Perform Accessing the RADIUS Server Administration Menu on page 97.

When and where to use: Optional if corrections are needed.

Procedure:

1. At the **Radius Server Administration** menu, enter the number associated with **Remove Radius Server Configuration**.

   A list of RADIUS servers is displayed:

   ```
   Configured Radius Servers
   ************************************
     1. Primary
     2. Secondary
     Select the type of radius server to remove (1-2):
   ```

   NOTICE: Only the existing, configured RADIUS servers are displayed.

2. Select the number associated with the server to remove.

   A warning message is displayed.

   ```
   ***WARNING***
   Removing server configuration for Secondary server will prevent
   future authentications from using this server
   Are you sure you want to continue (y/n) : y
   Radius server configuration successfully removed
   ```

   NOTICE: If an error message is displayed, the connection profile for that server must be removed first. See the delete function in Creating a Server Connection Profile on page 100.

3. Select `y` or `n` to confirm.
4. See other sections in this manual for adding, updating, and displaying RADIUS server configurations for corrections.

3.5.3.2.4
Updating a RADIUS Server Configuration

Prerequisites: Perform Accessing the RADIUS Server Administration Menu on page 97.

When and where to use: Optional if corrections are needed.

Procedure:

1. At the **Radius Server Administration** menu, enter the number associated with **Update Radius Server Configuration**.
2. Select the server at the prompt:

   ```
   Configured Radius Servers
   ************************************
     1. Primary
     2. Secondary
     Select the type of radius server to add (1-2):
   ```

   NOTICE: Only the existing, configured RADIUS servers are displayed.

3. Select the RADIUS server from the listed entries.
4. Enter the IP address or FQDN of the Radius Server.
5. Enter the RADIUS shared secret.

6 Enter the number of sockets.

The default value is provided in square brackets.

7 Verify the values displayed. Enter: `y` to confirm.

```
The following values will be set:
  Server: Secondary
  Address: 192.160.3.1
  Sockets: 100
  Secret: ********
Are you sure you want to continue (y/n/q) : y
Radius server configuration successfully added
```

8 See other sections in this manual for adding, removing, and displaying RADIUS server configurations for corrections.

3.5.3.2.5

Displaying a RADIUS Server Configuration

Prerequisites: Perform Accessing the RADIUS Server Administration Menu on page 97.

When and where to use: Optional: Display the RADIUS server configuration for verification.

Procedure:

1 At the **Radius Server Administration** menu, enter the number associated with **Display Radius Server Configuration**.

A short message is displayed:

```
The following values are currently configured
  Server: Primary
  Address: 192.160.3.1
  Sockets: 100
  Secret: ********
```

NOTICE: The secondary server is not configured in this example.

2 Optional: See other sections in this manual for adding, removing, and updating RADIUS server configurations for corrections.

3.5.3.2.6

Creating a Server Connection Profile

Perform this procedure to navigate to the IPsec Configuration menu from the main administration menu.

Prerequisites: See RADIUS Configuration for MVPN Servers on page 96.

Procedure:

1 Log in to the Mobile VPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `admin_menu`

3 At the **Main Menu**, enter the number associated with **Application Administration**.

4 At the **Application Administration** menu, enter the number associated with **IPsec Configuration**.

3.6
Device Connection Profiles Configuration

Clients connecting to the Motorola Solutions Mobile VPN Gateway must match a connection profile to connect.

Devices are typically maintained (added, modified, deleted) on a day-to-day basis. For a new installation, at least one device should be configured with a connection profile for verification of communications. See Creating Connection Profiles for the Mobile VPN Gateway on page 101 and Device Authentication Method Configuration on page 88 for the first device.

IMPORTANT: Import the certificate chains for both the primary and secondary gateways **before** creating a connection profile.

Connection profiles are defined on the gateway for the different classes of device or connection. These profiles describe parameters for the connection such as the transport security used for the connection, the protected networks a client is allowed to access, and the lifetime of the IPsec tunnel before it is renewed.

Connection profiles have one or more authentication mechanisms configured which are used for client authentication. Authentication mechanisms can be added and removed independently from connection profiles, but at least one authentication mechanism, to accept incoming connections, is necessary.

3.6.1
Creating Connection Profiles for the Mobile VPN Gateway

Device connection profiles are created. Authentication to the connection profile is added.

Prerequisites: Perform Device Authentication Method Configuration on page 88.

When and where to use: The configuration of a specific Motorola Solutions Mobile VPN Gateway is based on pre-defined profiles. Create a connection profile on each device and perform this procedure on the active MVPN Gateway.

NOTICE: This procedure supports OSPF for Public Safety LTE starting at release 11.0.

Procedure:

1. Log in to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **IPsec Configuration**.
5. At the **IPsec Configuration** menu, enter the number associated with **Create New Connection Profile**.
6. Select one of the following profiles.

   For each value entered, use the following definitions:

   - **CIDR (IPv4) format** - for the CIDR (IPv4) format, see your customer-specific IP planner. See the note at step 18 in Configuring the Network Identity on page 65 if needed.
   - **dpddelay** - DPD delay (minutes) stands for Dead Peer Detection delay. For more details, see *RFC 3706*.
   - **rightsourceip** - defines pool (or subnet) of IP addresses leased to VPN clients. The **rightsourceip** subnet is hidden to public Internet infrastructure but visible to peer in

protected enterprise network. Routing to the given **rightsourceip** subnet must point to floating Internal IP of MVPN Gateway which has connection profiles with this **rightsourceip** subnet.

- **leftsubnet** - usually defines static network destinations (in protected enterprise network) which VPN client needs to access via VPN tunnel. Destinations in **leftsubnet** are hidden to public Internet infrastructure. In addition, MVPN Gateway should have configured each destination from **leftsubnet** in VPN Internal Network Interface Routes list.

  NOTICE: For Remote Access profile, if UE has to connect to another device directly (SVOIP) within same or through another MVPN Gateway, the **leftsubnet** parameter should also include **rightsourceip** pool used by another UE devices.

- **rightsubnet** - defines static network destinations provided by Site-To-Site VPN clients. Destinations in **rightsubnet** are hidden to public Internet infrastructure but visible to peer in protected enterprise network. Routing to given **rightsubnet** destinations must point to floating Internal IP of MVPN Gateway which has connection profiles with these **rightsubnet** destinations.
- **right** - defines actual address of VPN client device, for example public Internet address granted by LTE infrastructure. Astro Site-To-Site profile uses this parameter to limit scope of public internet addresses of devices establishing VPN tunnel to MVPN Gateway.
- **rightid** - defines identity of client upon VPN authentication. For Certificate authentication, the **rightid** parameter is treated as “CA Subject DN” and can contain wildcard * character to match relative distinguished names (RDN). To match a wildcard template, the DN of a peer must contain the same number of RDNs in exact order defined by the “CA Subject DN” template. For the list of supported RDNs, see Profile Differentiation on page 134.
- **rightdns** - configures the VPN client to use application DNS servers (RED DNS) accessible via tunnel. Windows and Motorola MVPN (since PSLTE11) clients support this parameter. MVPN Gateway should have configured destination containing DNS server IP addresses from rightdns parameter in VPN Internal Network Interface Routes list. Also, rightdns ip addresses should be contained by subnet defined in **leftsubnet** parameter.
- **DSCP value** - QoS markup for outbound IKE packets only. Outbound IPsec packets with encrypted user data preserve QoS markup from original packets.

NOTICE: Default values are in square brackets “[ ]”.

If…	Then…
If you are using ASTRO Subscriber devices,	Perform the following actions: **a** Select the **Astro Subscriber** profile. **b** Enter the client tunnel IP address pool **(rightsourceip)** in the CIDR (IPv4) format. **c** Enter the DPD delay in minutes. **d** Enter the keying tries. **e** Enter the re-key margin in minutes. **f** Select a AES256-HEX pre-shared key.
If you are using LTE devices for remote access,	Perform the following actions: **a** Select the **Remote Access** profile when using single VPN entry point, or non-OSPF environment..

If…	Then…
and you are establishing a direct VPN tunnel between client and the MVPN Gateway, or a VPN tunnel between the MVPN Gateway and a VML750 if "LAN Mode" is configured in the "NAT" mode,	**b** Select the **OSPF Remote Access** profile when using multiple (for example, geographically redundant) VPN entry points and OSPF environment. **NOTICE:** Supporting OSPF Public Safety LTE starting at release 11.0. **c** Enter the client tunnel IP address pool **(rightsourceip)** in the CIDR (IPv4) format. **d** Enter left subnet (network/netmask) in the CIDR (IPv4) format. **e** Enter the DPD delay in minutes. **f** Enter IKE lifetime in hours. **g** Enable Rekeying (accept default value). **h** Enter the keying tries. **i** Enter the key life in hours. **j** Choose to enable or disable re-authorization. **k** Enter the re-key margin in minutes. **l** Enter IP address of DNS server to provide DNS configuration upon a request from client **(rightdns)**. **m** Enter DSCP value. **n** Choose the authentication type to add to the new connection profile. (Certificate based). **o** Select a chain of certificates from the list of configured chains. **p** Enter the right id (CA Subject DN with wildcards).
If you are using Windows client for remote access, **and you are establishing a direct VPN tunnel between client and the MVPN Gateway, using Active Directory (RADIUS) Authentication,**	Perform the following actions: **a** Select the **Remote Access** profile when using single VPN entry point, or non-OSPF environment.. **b** Select the **OSPF Remote Access** profile when using multiple (for example, geographically redundant) VPN entry points and OSPF environment. **NOTICE:** Supporting OSPF Public Safety LTE starting at release 11.0. **c** Enter the client tunnel IP address pool **(rightsourceip)** in the CIDR (IPv4) format. **d** Enter left subnet (network/netmask) in the CIDR (IPv4) format. **e** Enter the DPD delay in minutes. **f** Enter IKE lifetime in hours. **g** Disable Rekeying. **h** Enter the keying tries. **i** Enter the key life in hours.

If…	Then…
	j Disable re-authorization. **k** Enter the re-key margin in minutes. **l** Enter IP address of DNS server to provide DNS configuration upon a request from client **(rightdns)**. **m** Enter DSCP value. **n** Choose the authentication type to add to the new connection profile (Username-Password based). **o** Select a chain of certificates from the list of configured chains. **NOTICE:** The RADIUS server configuration is configured before adding “username-password” as the authentication type. **p** Enter the right id (CA Subject DN with wildcards).
If you are establishing a VPN tunnel between the MVPN Gateway and a VML750 that is configured in the router mode, **with a subnet associated with the connection that has “LAN Mode” configured in the “Mobile Router” mode,**	Perform the following actions: **a** Select the **Site to Site** profile when using single VPN entry point, or non-OSPF environment. **b** Select the **OSPF Site to Site** profile when using multiple (for example, geographically redundant) VPN entry points and OSPF environment. **NOTICE:** Supporting OSPF Public Safety LTE starting at release 11.0. **c** Enter left subnet (network/netmask) in the CIDR (IPv4) format. **d** Enter right subnet (network/netmask) in the CIDR (IPv4) format. **e** Enter the DPD delay in minutes. **f** Enter the IKE lifetime in hours. **g** Enter the keying tries. **h** Enter the key life in hours. **i** Choose to enable or disable re-authorization **(reauth)**. **j** Enter the re-key margin in minutes. **k** Enter IP address of DNS server to provide DNS configuration upon a request from client **(rightdns)**. **l** Enter the DSCP value. **m** Select a chain of certificates from the list of configured chains. **n** Enter the right id (CA Subject DN with wildcards).
If you are establishing a VPN tunnel between the MVPN Gateway and a Sierra GX450 modem,	Perform the following actions: **a** Select the **ASTRO Site-to-Site** profile. **b** Enter left subnet (network/netmask) in the CIDR (IPv4) format. Up to 3 subnet supported.

If…	Then…
	c Enter client IP address **(right)**. Acceptable values are %any, IP or CIDR (IPv4) format. **d** Enter right subnet (network/netmask) in the CIDR (IPv4) format. Up to 3 subnet supported. **e** Enter the DPD delay in minutes. **f** Enter the DPD timeout in minutes. **g** Enter the IKE lifetime in hours. **h** Enter the keying tries. **i** Enter the key life in hours. **j** Disable re-authorization. **k** Disable re-keying. **l** Enter the re-key margin in minutes. **m** Select a IKE1-PLAIN preshared-key.

3.6.1.1

Mobile VPN Topology

The following figures show how network parameters of different types of connection profiles map onto the Mobile VPN topology.

Figure 13: Remote Access and ASTRO Subscribers Mobile VPN Topology

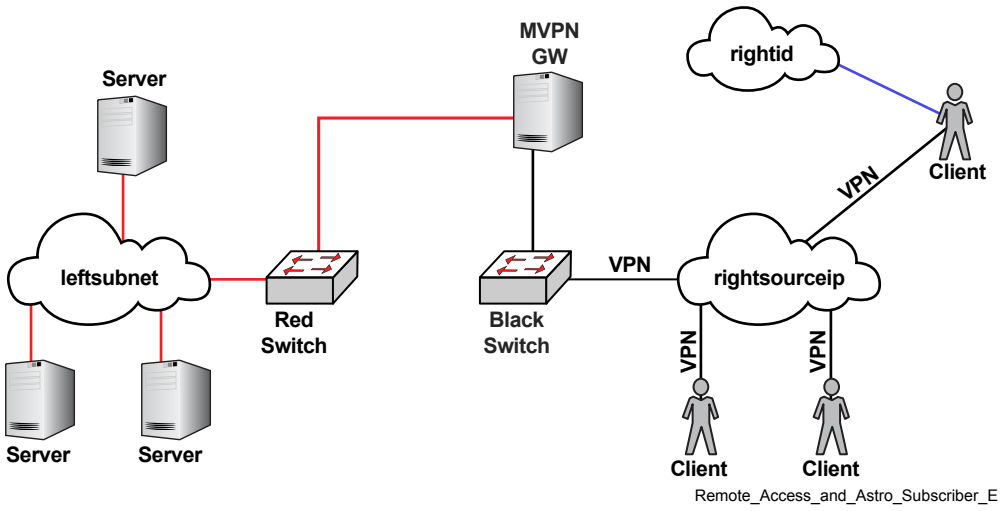
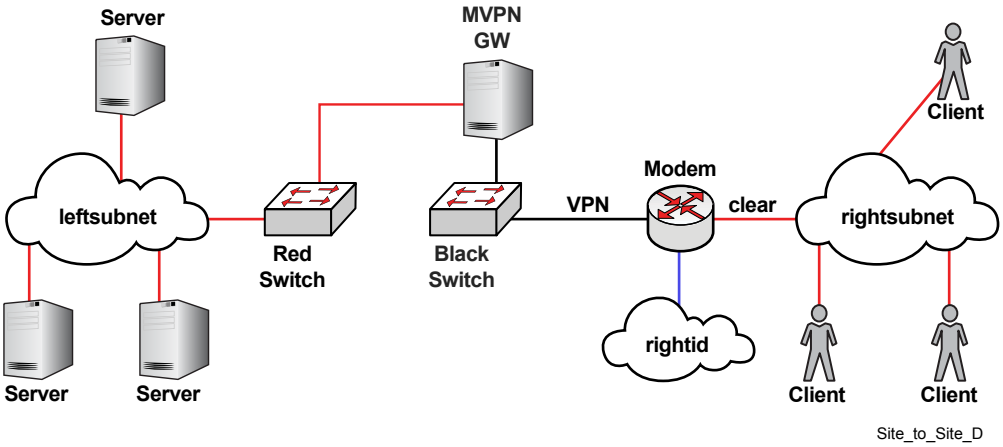


Figure 14: Site-to-Site Mobile VPN Topology



3.6.2

Updating the Connection Profile

Change and update the values for a selected connection profile.

When and where to use: Perform this procedure on the active Motorola Solutions Mobile VPN Gateway.

Procedure:

1. Log in to the MVPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.

2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **IPsec Configuration**.
5. At the **IPsec Configuration** menu, enter the number associated with **Update Connection Profile**.
6. An interactive script runs. Answer the prompts. Select an available connection profile from the list displayed.

   Default values are in square brackets "[ ]".

   Step example:

```
  1. Astro_Subscriber-1

Select Connection Profile (1-1): 1
Enter dpddelay in minutes (5m-60m) [6m]: 5m
Enter keyingtries (1-10)[4]: 3
Enter rekeymargin in minutes (1m-9m) [4m]: 3m
```

3.6.3
Deleting the Connection Profile

Delete a selected connection profile.

When and where to use: Perform this procedure on the active Motorola Solutions Mobile VPN Gateway.

Procedure:

1. Log in to the MVPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **IPsec Configuration**.
5. At the **IPsec Configuration** menu, enter the number associated with **Delete Connection Profile**.
6. An interactive script runs. Answer the prompts. Select an available connection profile from the list displayed.

   Step example:

```
  1. Astro_Subscriber-1
  q. Quit
Select the connection profile to remove (1-1,q): 1

WARNING: The following authentication mechanisms are still
configured for the selected connection profile.  Clients
will no longer be able to connect to the VPN gateway using
these methods if this connection profile is removed:
  dev@key1-aes256

Deleting this connection profile will also disconnect
0 active Security Association(s)
Continue with connection profile deletion? (y/n): y

Removed Connection Profile: Astro_Subscriber-1
```

3.6.4
Displaying the Connection Profile Information

Display a selected connection profile.

When and where to use: Perform this procedure on the active Motorola Solutions Mobile VPN Gateway.

Procedure:

1. Log in to the MVPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **IPsec Configuration**.

5 At the **IPsec Configuration** menu, enter the number associated with **Display Connection Profile Information**.

6 An interactive script runs. Answer the prompts. Select an available connection profile from the list displayed.

Step example:

```
  1. Astro_Subscriber-1
  q. Quit
Select Connection Profile to view details (1-1,q): 1
Astro_Subscriber-1
---------------------------------------
rightsourceip: 192.162.101.0/24
dpddelay: 5m
keyingtries: 3
rekeymargin: 3m
Authentication mechanisms assigned to profile:
dev@key1-aes256
```

3.6.5
Adding Authentication to a Profile

Authentication is added to the selected profile.

When and where to use:
Perform this procedure on the active Motorola Solutions Mobile VPN Gateway.

Perform Creating Connection Profiles for the Mobile VPN Gateway on page 101.

Procedure:

1 Log in to the MVPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `admin_menu`

3 At the **Main Menu**, enter the number associated with **Application Administration**.

4 At the **Application Administration** menu, enter the number associated with **IPsec Configuration**.

5 **NOTICE:** Corresponding certificate chains must be imported to the redundant Mobile VPN GW before creation of the connection profile **with the same name**.

At the **IPsec Configuration** menu, enter the number associated with **Add Authentication to Connection Profile**.

6 Select a connection profile.

7 Select a pre-shared key (applies to systems that include an ASTRO® 25 network or pre-shared key supporting devices), certificate chain or certificate chain with User-Password authentication (applies to Remote Access profiles supporting Microsoft Windows clients).

3.6.6
Removing Authentication from a Profile

When and where to use: Perform this procedure on the active Motorola Solutions Mobile VPN Gateway.

Procedure:

1 Log in to the MVPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `admin_menu`

3 At the **Main Menu**, enter the number associated with **Application Administration**.

4 At the **Application Administration** menu, enter the number associated with **Configuration**.

5 At the **IPsec Configuration** menu, enter the number associated with **Remove Authentication from Connection Profile**.

6 Select a connection profile.

7 Select authentication to remove, by entering the number associated with the pre-shared key (applies to systems that include an ASTRO® 25 network or pre-shared key supporting devices), certificate chain or User-Password authentication (applies to Remote Access profiles supporting Microsoft Windows clients).

8 To continue with authentication removal, enter: `Y`

The selected profile is removed successfully.

3.6.7
Setting Global Parameters for Connection Profiles

Prerequisites: Perform Defining the Cluster on page 72.

When and where to use:
This procedure shows how to set various strongSwan values. See Certificate Revocation List (CRL) on page 33.

Some of the strongSwan Global Values included, but not limited to, are:

- Enable or disable ESP Suites(s).
- Enable or disable IKE Suites(s).
- “CRL Enforcement Policy” – Defines if the client certificate checked against the Certificate Revocation List (CRL) is: required, not expected or optional.
- To connect from **Windows**, the following should be enabled:
  - IKE Suite aes256-sha384-prfsha384-modp1024
  - ESP suite aes256-sha1 or aes256-sha1-modp1024
- To connect from **Astro Site-To-Site** device, the following should be enabled:
  - IKE Suite aes256-sha1-modp1024
  - ESP suite aes256-sha1-modp1024

Procedure:

1 Log in to the Mobile VPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `admin_menu`

3 At the **Main Menu**, enter the number associated with **Application Administration**.

4 At the **Application Administration** menu, enter the number associated with **IPsec configuration**.

5 At the **IPsec Configuration** menu, enter the number associated with **Set Strongswan Global Values**.

6 An interactive script runs. Answer the prompts. Select according to your customer-specific plan.

Default values are in square brackets “[ ]”. The example shows the default selections for MVPN.

Step example:

```
 [X] 1. aes256gcm16-ecp384
 [X] 2. aes256gcm16
 [X] 3. aes256-sha1-modp1024
 [X] 4. aes256-sha1
     d. Done
Select ESP Suites(s) to enable/disable (1-4,d): d

 [X] 1. aes256-sha384-prfsha384-ecp384
 [X] 2. aes256-sha384-prfsha384-modp1024
     d. Done
Select IKE Suites(s) to enable/disable (1-2,d): d

Enter the message retransmit exponential backoff factor (1.0-2.0)
[1.0]:
Enter the message retransmit timeout in seconds (10-60)[15]:
Enter the number of message retransmit attempts (2-10)[4]:
Enter the crl enforcement policy (yes|no|ifuri) [no]:
------------------------------------------------------------------------
-----------
The following parameters will be changed:
ESP Suite: aes256gcm16-ecp384,aes256gcm16
IKE Suite: aes256-sha384-prfsha384-ecp384
Message Retransmit Base: 1.0
Message Retransmit Timeout: 15 seconds
Message Retransmit Attempts: 4
CRL Policy: no
------------------------------------------------------------------------
-----------
Is this correct (y/n, q) : y

Modifications will take effect at the next VPN restart.
```

Chapter 4

Mobile VPN Gateway Operations

4.1 Logging on to the Mobile VPN Gateway

Prerequisites: PuTTY is loaded on the Windows based local machine. See Installing VMware PowerCLI and PuTTY on page 155.

Procedure:

1. Launch PuTTY with the icon or shortcut configured at installation.
2. In the host name field, enter the ***<username>***`@`***<the IP associated with eth0>***

   For the IP address, see Configuring the Network Identity on page 65.

   Step example: `ipsecadm@192.162.0.33`
3. Check the SSH box under **Connection type:**.
4. Ensure that the Port field is set to 22.
5. Click **Open**.
6. Type the MVPN Gateway password at the console window.

4.2 Logging off from the Mobile VPN Gateway

When and where to use: Log off from various network tools, such as vSphere Client and PuTTY.

NOTICE: For a complete (clean) console window log off, exit any application that is running in the console window, such as an interactive menu. The **exit** command works in several network tool applications to close a console connection.

Procedure:

1. In the **Console** window, type `exit`
2. Close the **vSphere Client** window (or other network tool application window interface).

4.3 Changing the ESXi User Password

Follow this procedure to change the ESXi root user password. For security reasons, it is recommended to change the password every 30 days.

IMPORTANT: Different root passwords on ESXi1 – NMHOST01 and ESXi2 – NMHOST02 are supported. For security reasons, set a different password on each server.

Procedure:

1. Launch the **VMware vSphere Client** from the Windows-based device where it resides.

   A desktop shortcut was created during installation.
2. Log on to the server as `root`.

   The **vSphere Client Inventory** window appears.

3 Select the server from the pane on the left and click the **Local Users & Groups** tab for this server.

4 In the **Local Users & Groups** tab, perform the following actions:

   a Right-click the user whose password you want to change.

   b From the pop-up menu, select **Edit**.

5 In the **Edit User** window, perform the following actions:

   a Select the **Change password** check box.

   b In the **Password** field, type the new password.

   c In the **Confirm** field, retype the new password.

   d Click **OK**.

4.4 Shutting Down the Mobile VPN Gateway Virtual Machine

Procedure:

In the **vSphere Client** window, in the pane on the left, right-click the Virtual Machine you want to shut down and select **Power** → **Shut Down Guest**.

4.5 Mounting a Drive in vSphere Client

Prerequisites: The procedure, Installing the VMware vSphere Client on Windows-Based Computer on page 158 has been performed.

When and where to use: To access a physical or virtual drive on the local machine.

Procedure:

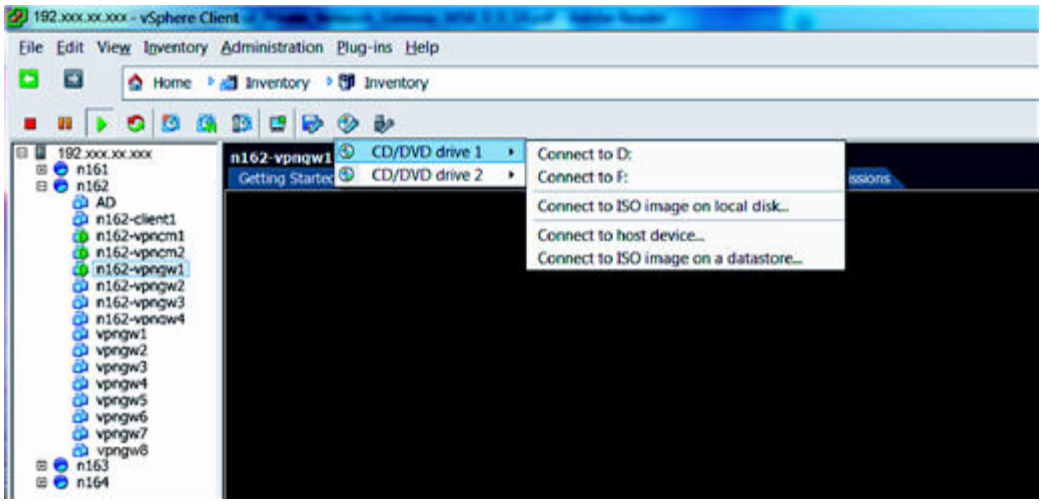
1 Launch the **VMware vSphere Client** and login. See Logging On to the VMware vSphere Client on page 53.

2 In the navigation pane of the **VMware vSphere Client** main window, select a Linux-based virtual machine.

3 To mount a drive in vSphere client, click the **drive** icon in the inventory window, as shown in Figure 15: Drive Selection in vSphere Client on page 113. Select the drive desired and the location of the CD/DVD optical drive or file path for an iso file.

   This action mounts the drive.

Figure 15: Drive Selection in vSphere Client



4.6

Unmounting a Drive in vSphere Client

Perform this procedure to release access for a physical or virtual drive on the local machine.

Prerequisites:
Perform Installing the VMware vSphere Client on Windows-Based Computer on page 158.

Perform Importing OVF into Virtual Server on page 55.

Procedure:

1. Launch the **VMware vSphere Client** and login.

   See Logging On to the VMware vSphere Client on page 53.

2. In the navigation pane of the **VMware vSphere Client** main window, select a Linux-based virtual machine.

3. Perform one of the following:

If…	Then…
Configuring the Network Identity on page 65 has not been performed,	**a** Select the **Console** tab for the selected virtual machine. **b** Log on as the `root` user. **c** Continue with step 4.
Configuring the Network Identity on page 65 has been performed,	**a** Perform Logging on to the Mobile VPN Gateway on page 111 **b** Continue with step 4.

4. At the command prompt, enter: `admin_menu`

5. At the **Main Menu** prompt, enter the number associated with `OS Administration`.

```
Main Menu (* - Option not available)
**************************************
  1. Software Administration
  2. OS Administration
  3. Services Administration
```

```
  4. Backup and Restore Administration
  5. Application Administration
  q. Quit
Enter selection (1-5,q): 2
```

6 At the **OS Administration** menu, select the number associated with `Eject CD/DVD`.

7 At the **Eject CD/DVD** menu, select the number associated with the option desired.

If media exists, and is recognized, it is listed in the `Eject CD/DVD` menu.

Step example: This example is shown for `cdrom1`.

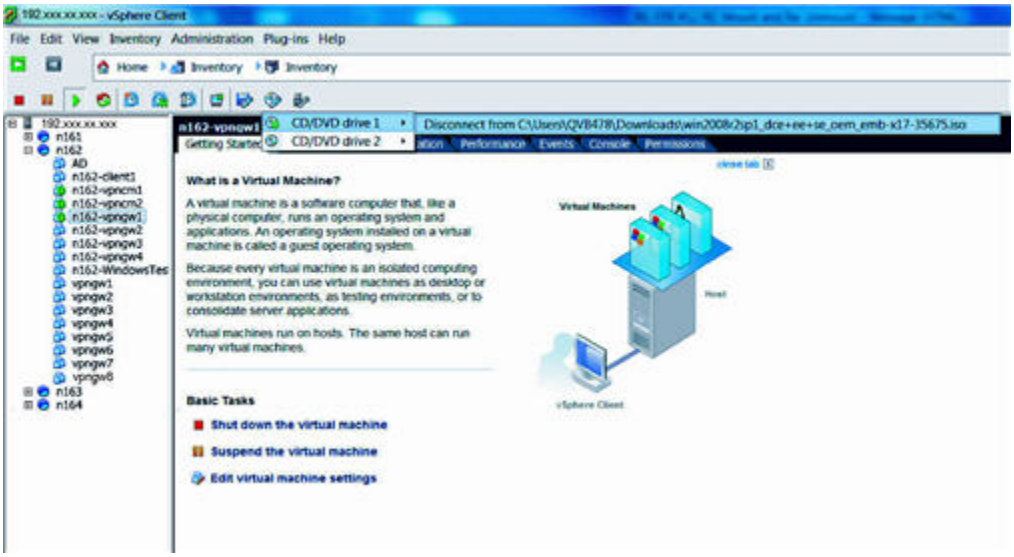
```
Eject CD/DVD
**************************************
  1. cdrom0 (*No media present*)
  2. cdrom1 (GRMSXFREO_EN_DVD)
  3. Eject All
  b. Back to Previous Menu
  q. Quit
Enter selection (1-3,b,q): 2

Ejecting cdrom1

Please remove media and press <ENTER> to continue.
```

8 In vSphere client, click the **drive** icon in the inventory window, as shown in the figure. Select the drive desired and **Disconnect from***<name of the image mounted to that drive>* from the menu, as shown in Figure 16: Drive Selection in vSphere Client on page 114.

Figure 16: Drive Selection in vSphere Client



9 At the command prompt, press ENTER.

4.7 Manage the Mobile VPN Gateway Administrative User Accounts

The required administrative user accounts are created automatically during system installation. They are pre-configured with the system default password. These passwords should be changed at the earliest opportunity for security reasons.

Two of these accounts, `fencing` and `clusync` are managed using the admin_menu. See Changing the Fencing Password on page 76 and Accessing the Clusync User Credentials Menu on page 77 in the Manage the VPN Cluster on page 71 section of this manual.

4.7.1
Operations on Local Users

Use these procedures to create and maintain local user accounts required for your organization. These procedures are not for Motorola Solutions Mobile VPN Gateways joined to Domain Controllers. The Domain Controller has users configured for use by the Mobile VPN Gateway. See Joining the Mobile VPN Gateway to an Existing Domain Controller on page 67 in this manual.

To create and maintain local user accounts, refer to the following sections:

- Creating a Local User on page 115
- Modifying a Local User on page 116
- Deleting a Local User on page 117

An exhaustive explanation of Linux commands is not included in this manual. Use a Linux reference, or the various help functions in Linux, such the command man pages, for details of command line entries.

By changing directories to `/usr/local/home`, one can see the current list of local users on the MVPN Gateway.

4.7.1.1
Creating a Local User

Prerequisites: Ensure the new user does not exist on a Domain Controller joined with the MVPN Gateway. See Operations on Local Users on page 115.

When and where to use: Perform this procedure to create local user accounts.

Procedure:

1 Log in to the Mobile VPN Gateway as the `root` user.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter:
`useradd -d /usr/local/home/`***`<username>`*** `-g` ***`<group>`***`-m -u` ***`<uid>`*** `–G` ***`<list of secondary groups><username>`***

Where:

`<username>` is the new user account login name

`<uid>` is the numerical value of the new user

`<group>` is the group name for the user initial login group

`<list of secondary groups>` is the list of supplementary groups

Rules for the user name are:

- Maximum length 32 characters
- No spaces
- Alphabetic first character
- Underscore may be included

Four user names are defined as roles. Each is assigned an initial group, and secondary groups. These user names (roles) are:

- ipsecadm
- ipsecmgr
- clusync
- hafence

For initial groups and secondary groups:

- Initial and secondary groups are: domuser, instadm, platadm, infradm, secadm, auditors, subssec, bkupadm, netwadm
- Secondary groups are entered as a list with comma separators.

Step example:

```
useradd -d /usr/local/home/ipsecadm -g domuser -m -u 1055 –G
instadm,platadm,infradm,secadm,auditors,subssec,bkupadm,netwadm
ipsecadm
```

3 At the command prompt, enter: `passwd` ***<username>***

NOTICE:
All passwords must meet the following criteria:

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

4 At the prompt, enter the new password for the new ***<username>*** user account.

5 Enter the new password when prompted again.

4.7.1.2
Modifying a Local User

Prerequisites:

- The local user account exists.
- Determine the user to be modified, and what must be modified for that user.
- Ensure the user is not logged in, or performing a function, such as running a crontab, script, or spooling a print job.

NOTICE: This procedure shows examples to lock the user and change groups. Other modifications, such as changing the user name are possible. See Operations on Local Users on page 115.

When and where to use: Perform this procedure to modify local user accounts. Typical modifications to a user account include moving the user account, assigning different groups to the user account and locking the user account. Other options are available in the procedure below.

NOTICE: See Creating a Local User on page 115 for a listing of the main users and groups used in the MVPN Gateway.

Procedure:

1 Log in to the Mobile VPN Gateway as the `root` user.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `usermod –L` ***<username>*** to lock the user password.

Step example: `usermod –L joe5`

3 At the command prompt, enter: `usermod –U` ***<username>*** to unlock the user password.

Step example: `usermod –U joe5`

4 At the command prompt, enter: `usermod –g` ***<group><username>*** to change the initial group the user is associated with.

NOTICE: The group used in this command overwrites the existing initial group the user is associated with. This may be a duplicate of the secondary group the user is associated with. This may not be desired.

Step example: `usermod –g domuser joe5`

5 At the command prompt, enter: `usermod –G` ***<list of secondary groups><username>*** to change the list of secondary groups the user is associated with.

NOTICE: The groups listed in this command replace the existing groups the user is associated with. If it is desired to simply add new group to the user, the existing set of groups must be entered in this command.

Step example: `usermod –G infradm,secadm,auditors joe5`

4.7.1.3
Deleting a Local User

Prerequisites:

- The local user account exists.
- Determine the user to be deleted.
- Ensure the user is not logged in, or performing a function, such as running a crontab, script, or spooling a print job.
- Refer to the Linux help and man pages for removal activities associated with the user, such as user files.

When and where to use: Perform this procedure to delete local user accounts, and any files associated with the user account.

NOTICE: See Creating a Local User on page 115 for a listing of the main users and groups used in the MVPN Gateway.

CAUTION: Certain system variables in `/etc/login.defs` may cause unexpected results. Deleting the user using the `–f` option may also delete the group associated with the user. This may not be desired. Use a Linux reference, or the various help functions in Linux, such the command man pages, for details of command line entries.

Procedure:

1 Log in to the Mobile VPN Gateway as the `root` user.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `userdel –f` ***<username>*** to force the deletion of the user.

Step example: `userdel –f joe5`

4.7.2
Changing the ipsecmgr Password

Procedure:

1 Log in to the MVPN Gateway as the `ipsecmgr` user. .

2 At the command prompt enter `passwd`

a At the UNIX password prompt, enter the current password for the ipsecmgr account.

b At the New password prompt, enter the new ipsecmgr password.

c At the Retype new password prompt, reenter the new ipsecmgr password.

If the password is unacceptable or if the re-entry of the password does not match the original entry, the error message appears prompting user to take corrective action.

If no errors are printed, the message `passwd: all authentication tokens updated successfully` appears. You may be logged out of the system.

4.7.3
Changing the ipsecadm Password

Procedure:

1. Log in to the MVPN Gateway as the `ipsecadm` user. Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt enter `passwd`
   - **a** At the UNIX password prompt, enter the current password for the ipsecadm account.
   - **b** At the New password prompt, enter the new ipsecadm password.
   - **c** At the Retype new password prompt, reenter the new ipsecadm password.

   If the password is unacceptable or if the re-entry of the password does not match the original entry, the error message appears prompting user to take corrective action.

   If no errors are printed, the message `passwd: all authentication tokens updated successfully` appears. You may be logged out of the system.

4.7.4
Changing the root Password

Procedure:

1. Log in to the MVPN Gateway as the `root` user.
2. At the command prompt enter `passwd root`
   - **a** At the New password prompt, enter the new root password.
   - **b** At the Retype new password prompt, reenter the new root password.

   If the password is unacceptable or if the re-entry of the password does not match the original entry, the error message appears prompting user to take corrective action.

   If no errors are printed, the message `passwd: all authentication tokens updated successfully` appears. You may be logged out of the system.

4.8
High Availability Administration

With the High Availability option, it is possible to turn off a primary Motorola Solutions Mobile VPN Gateway while retaining the Mobile VPN Gateway service. The backup Mobile VPN Gateway takes

over automatically. Both Mobile VPN Gateways must be online for such operation; to determine their status see Displaying the Mobile VPN Gateway Availability Status on page 120.

4.8.1
Setting the Mobile VPN Gateway Node Online

Prerequisites: Check the Motorola Solutions Mobile VPN Gateway availability status. See Displaying the Mobile VPN Gateway Availability Status on page 120.

Procedure:

1. Log in to the MVPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **High Availability Administration**.
5. At the **High Availability Administration** menu, enter the number associated with **Set VPN Gateway Online**.

   The warning message appears.
6. Enter: `Y`

   The Mobile VPN Gateway is set online.

4.8.2
Setting the Mobile VPN Gateway Node Offline

IMPORTANT: Setting off the Motorola Solutions Mobile VPN Gateway node offline, turns off IPsec service if the backup node is not running.

Prerequisites: Check the Mobile VPN Gateway availability status. See Displaying the Mobile VPN Gateway Availability Status on page 120.

Procedure:

1. Log in to the MVPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **High Availability Administration**.
5. At the **High Availability Administration** menu, enter the number associated with **Set VPN Gateway Offline**.

   The warning message appears.
6. Enter: `Y`

   The Mobile VPN Gateway is set offline.

4.8.3
Displaying the Mobile VPN Gateway Availability Status

Procedure:

1. Log in to the MVPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **High Availability Administration**.
5. At the **High Availability Administration** menu, enter the number associated with **Display VPN Gateway Availability Status**.

   The cluster status is displayed.

4.8.4
Verifying the Mobile VPN Gateway Availability Status

To verify the configuration, check the status of the gateway clusters (nodes) and gateway availability status.

The status of the gateway clusters (nodes) are:

- For redundant configuration, one node should be `ONLINE ACTIVE`, the other `ONLINE STANDBY`
- For non-redundant configuration, the First Node should be `ONLINE ACTIVE`, the Second Node `INACTIVE`

The gateway availability status should be `ONLINE` or `INACTIVE`.

Process:

1. Verify the SSH connectivity.

   See Checking SSH Connectivity on page 77.
2. Display clusters and cluster status.

   See Displaying the Cluster and Status on page 74.
3. Display the MVPN Gateway availability status.

   See Displaying the Mobile VPN Gateway Availability Status on page 120.

4.9
Manage SNMP Authentication

This section provides information for the management of the SNMP authentication on the MVPN Gateway for local servers only. Following SNMP users are preconfigured in Mobile VPN Gateway:

Table 13: Mobile VPN Gateway SNMP Users

User Name	Default Access	Purpose
MotoAdmin	Auth, Privacy	Managed SNMP configuration for local users
MotoNorth-Motorola	No Auth, No Privacy	Provides authentication for SNMPv3 Discovery and Access

Table continued…

User Name	Default Access	Purpose
MotoInformA	No Auth, No Privacy	Provides authentication for SNMPv3 Inform Trap

4.9.1
Setting SNMP Authentication

Prerequisites: The set identity procedure has been performed on virtual machines of the MVPN gateways cluster. This is done during Configuring Virtual Machine Security Settings on page 61 by performing Configuring the Network Identity on page 65.

When and where to use:
Use this procedure to change the Authentication and Privacy passphrases used to authenticate access to machine SNMP agent from servers such as UEM or Genesis (applies to local servers only).

Procedure:

1. Log in to the Mobile VPN Gateway as the `ipsecadm` user.

   See Logging on to the Mobile VPN Gateway on page 111.

2. At the command prompt, enter **admin_menu**
3. At the **Main Menu** prompt, enter number associated with **OS Administration**.
4. At the **OS Administration** prompt, enter number associated with **Security Provisioning**.
5. At the **Security Provisioning** prompt, enter number associated with **Manage SNMP Passphrases**.
6. At the **Manage SNMP Passphrases** prompt, enter number associated with **Configure SNMPv3 Agent**.
7. At the **MotoAdmin Authentication Passphrase** prompt, enter MotoAdmin SNMP user authentication passphrase.
8. At the **MotoAdmin Privacy Passphrase** prompt, enter MotoAdmin SNMP user privacy passphrase.

   Step example: If provided passphrases are correct, user gets access to SNMP Administration menu.

```
Manage SNMP Passphrases (* - Option not available)
**************************************
1. Configure SNMPv3 Agent
b. Back to Previous Menu
q. Quit
Enter selection (1,b,q): 1
Initializing SNMP Configuration Utility
MotoAdmin credentials are required to operate this utility.

MotoAdmin Authentication Passphrase : ****************
MotoAdmin Privacy Passphrase : ****************

SNMP Administration
===================
1. Modify SNMP User Configuration
2. Modify SNMP Inform Configuration
Select (1-2, q, ?) [q]:
```

9. At the **SNMP Administration** menu, enter number associated with **Modify SNMP User Configuration**.
10. At the **Select User to Modify** menu, select number associated with required user.

11 At the **MotoAdmin Authentication Passphrase** prompt, enter current MotoAdmin SNMP user authentication passphrase.

12 At the **MotoAdmin Privacy Passphrase** prompt, enter current MotoAdmin SNMP user privacy passphrase.

13 At the **<UserName> Authentication Passphrase** prompt, enter new authentication passphrase. Confirm new Authentication Passphrase by entering same value in next prompt.

14 At the **<UserName> Privacy Passphrase** prompt, enter new privacy passphrase. Confirm new Privacy Passphrase by entering same value in next prompt.

The following example demonstrates user steps done for changing MotoAdmin user passphrases.

Step example:

```
SNMP Administration
===================
 1. Modify SNMP User Configuration
 2. Modify SNMP Inform Configuration
Select (1-2, q, ?) [q]: 1

Select User to Modify
=====================
 1. MotoAdmin       AuthPriv
 2. MotoNorthMotorola      NoAuthNoPriv
Select (1-2, q, ?) [q]: 1

Select Modification
===================
For User: MotoAdmin AuthPriv
 1. Update Passphrases
Select (1, q, ?) [q]: 1
Enter current MotoAdmin Authentication Passphrase : ****************
Enter current MotoAdmin Privacy Passphrase : ****************
Enter new MotoAdmin Authentication Passphrase : ****************
Confirm new MotoAdmin Authentication Passphrase : ****************
Enter new MotoAdmin Privacy Passphrase : ****************
Confirm new MotoAdmin Privacy Passphrase : ****************
Success : Change MotoAdmin Authentication Passphrase
Success : Change MotoAdmin Privacy Passphrase
Success : Commit data

Operation Succeeded.
```

4.9.2
Changing SNMP Authentication and Privacy Level

Prerequisites: The set identity procedure has been performed on virtual machines of the MVPN gateways cluster. This is done during Configuring Virtual Machine Security Settings on page 61 by performing Configuring the Network Identity on page 65.

When and where to use:
Use this procedure to change the Authentication and Privacy authentication level to machine SNMP agent from servers such as UEM or Genesis (applies to local servers only).

Procedure:

1 Log in to the Mobile VPN Gateway as the `ipsecadm user`.

See Logging on to the Mobile VPN Gateway on page 111.

2 At command prompt, enter **admin_menu**

3 At **Main Menu** prompt, enter number associated with **OS Administration**.

4 At **OS Administration** prompt, enter number associated with **Security Provisioning**.

5 At **Security Provisioning** prompt, enter number associated with **Manage SNMP Passphrases**.

6 At **Manage SNMP Passphrases** prompt, enter number associated with **Configure SNMPv3 Agent**.

7 At **MotoAdmin Authentication Passphrase** prompt, enter MotoAdmin SNMP user authentication passphrase.

8 At **MotoAdmin Privacy Passphrase** prompt, enter MotoAdmin SNMP user privacy passphrase.

Step example: If provided passphrases are correct, user obtains access to **SNMP Administration** menu.

```
Manage SNMP Passphrases (* - Option not available)
**************************************
1. Configure SNMPv3 Agent
b. Back to Previous Menu
q. Quit
Enter selection (1,b,q): 1
Initializing SNMP Configuration Utility
MotoAdmin credentials are required to operate this utility.

MotoAdmin Authentication Passphrase : ****************
MotoAdmin Privacy Passphrase : ****************

SNMP Administration
===================
1. Modify SNMP User Configuration
2. Modify SNMP Inform Configuration
Select (1-2, q, ?) [q]:
```

9 At **SNMP Administration** menu, enter number associated with **Modify SNMP User Configuration**.

10 At **Select User to Modify** menu, select number associated with required user.

11 At **Enter New Security Level**, select number associated with new required level.

12 At **<UserName> Authentication Passphrase** prompt, enter new authentication passphrase. Confirm new Authentication Passphrase by entering same value in next prompt.

13 At **<UserName> Privacy Passphrase** prompt, enter new privacy passphrase. Confirm new Privacy Passphrase by entering same value in next prompt.

14 At **MotoAdmin Authentication Passphrase** prompt, enter current MotoAdmin SNMP user authentication passphrase.

15 At **MotoAdmin Privacy Passphrase** prompt, enter current MotoAdmin SNMP user privacy passphrase.

The following example demonstrates user steps done for changing MotoNorthMotorola user configuration from NoAuthNoPriv level to AuthPriv level.

Step example:

```
Select User to Modify
=====================
 1. MotoAdmin       AuthPriv
 2. MotoNorthMotorola NoAuthNoPriv
Select (1-2, q, ?) [q]: 2

Enter New Security Level
========================
For User: MotoNorthMotorola NoAuthNoPriv
```

```
 1. AuthNoPriv
 2. AuthPriv
Select (1-2, q, ?) [q]: 2
Enter new MotoNorthMotorola Authentication Passphrase :
****************
Confirm new MotoNorthMotorola Authentication Passphrase :
****************
Enter new MotoNorthMotorola Privacy Passphrase : ****************
Confirm new MotoNorthMotorola Privacy Passphrase : ****************
Enter MotoAdmin Authentication Passphrase : ****************
Enter MotoAdmin Privacy Passphrase : ****************
Success : Check response time
Success : Delete MotoNorthMotorola
Success : Remove VACM for MotoNorthMotorola
Success : Create MotoNorthMotorola
Success : Add VACM for MotoNorthMotorola
Success : Change MotoNorthMotorola Authentication Passphrase
Success : Change MotoNorthMotorola Privacy Passphrase
Success : Activate MotoNorthMotorola
Success : Commit data
```

Chapter 5

Mobile Virtual Private Network Gateway Maintenance

This chapter provides information and activities associated with the Motorola Solutions Mobile VPN Gateway (MVPN GW) server maintenance.

MVPN GW solution provides mechanism for manual and automatic backup creation of server configuration. Manual backup assumes logging in to MVPN server, initiating backup operation from the admin menu and perform a manual download of backup file to secure location. Automatic backup is used with ESU solution and this software manages backup creation and their transfer automatically.

Backup file contains configuration for entire MVPN GW cluster. The following configuration elements are included into the backup:

- IPsec general and user profile configuration
- Certificate chains with private keys
- PSK passphrases
- Iptables bypass rules
- Network configuration such as routing and network adapter settings
- SNMP access configuration

During backup and restore operations all MVPN GW servers must available. Restoration or backup of single, or selected number of MVPN GW servers is not supported.

5.1 Manually Backing Up all Mobile Virtual Private Network Gateway Cluster Configuration

Prerequisites:

- MVPN gateways cluster is functioning.
- OVF files are deployed on the virtual machines of the MVPN gateways cluster. This is done during Mobile VPN Gateway Installation on page 39 by performing Importing OVF into Virtual Server on page 55 and Verifying Import of the OVF into Virtual Server on page 57.
- The set identity procedure has been performed on virtual machines of the MVPN gateways cluster. This is done during Mobile VPN Gateway Configuration on page 61 by performing Configuring the Network Identity on page 65.
- The set cluster procedure has been performed on the `vpngw1` virtual machine (gateway). This is done during Mobile VPN Gateway Configuration on page 61 by performingDefining the Cluster on page 72.
- You have obtained removable media (secure USB or CD/DVD).

When and where to use: Create a backup file and a copy of the file for the MVPN gateway.

IMPORTANT: The backup function is run from the virtual machine, `vpngw1`. If the backup is run from another virtual machine, an error message is displayed, informing the user that backup must be performed from `vpngw1`. With the error message, no backup files are created.

Procedure:

1. Log in to the Mobile VPN Gateway (`vpngw1`).

   See Logging on to the Mobile VPN Gateway on page 111.

2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Backup and Restore Administration**.
4. At the **Backup and Restore Administration** menu, enter the number associated with **Backup**.

   Step example: The backup function output messages display:

   ```
   Getting cluster files, this may take a while...
   Created /var/opt/perstore/cluster-20140805094636.tar.gz
   Created archive file: /var/opt/perstore/restore/
   all-20140805094636.tar.gz
   ```

   NOTICE: If one of the virtual machine gateways in the cluster is powered off, or otherwise inaccessible, the backup fails and an error message is displayed. Changes are not applied. Correct the situation and repeat this procedure. A warning message is sent to syslog in: `/var/log/messages`

5. Record the file names created in the previous step.
6. A backup file is created as a compressed Linux tar file (`*.tar.gz` archive) and stored in the `/var/opt/perstore/restore/` directory.

   Using SFTP, the user creates a local file (copy) of the current archive files (see previous step) and saves the files to removable media (secure USB or CD/DVD).

7. Store the backup file media in a secure location.

5.2 Backup Support for Backup Manager Server

Perform procedures in this section to perform manual backup creation for the server configuration.

5.2.1 Performing On Demand Backup for MVPN Gateway Cluster

Prerequisites:

- MVPN gateways cluster is functioning.
- OVF files are deployed on the virtual machines of the MVPN gateways cluster. This is done during Mobile VPN Gateway Installation on page 39 by performing Importing OVF into Virtual Server on page 55 and Verifying Import of the OVF into Virtual Server on page 57.
- The set identity procedure has been performed on virtual machines of the MVPN gateways cluster. This is done during Mobile VPN Gateway Configuration on page 61 by performing Configuring the Network Identity on page 65.
- The set cluster procedure has been performed on the `vpngw1` virtual machine (gateway). This is done during Mobile VPN Gateway Configuration on page 61 by performing Defining the Cluster on page 72.
- The MVPN vpngw1 virtual server has been configured with correct address of backup manager server. To configure the MVPN server, perform Configuring the Network Identity on page 65.

- Routing to subnet containing UIS server is configured on vpngw1 machine. This is done by performing Configuring Management Network Routing for OSP Services, System Restore and Remote Access on page 80.
- Backup agent software on MVPN vpngw1 server is connected and registered on backup manager server.

When and where to use:
Perform backup of MVPN Gateway with centralized backup and restore management feature.

Procedure:

1. In a web browser recommended by *Operations Support Platform Backup Manager Operator Guide*, open the web address for the backup manager server.
2. Log on to backup manager server with the Backup role selected.

   NOTICE: User can execute Restore operation on backup manager console for MVPN GW. The backup manager server restore operation doesn't perform any restore of MVPN Gateway configuration. To perform restore follow the procedure **Recovering the Mobile VPN Gateway on page 167**.
   When MVPN GW backup file is downloaded directly from backup manager server, use zip archiver utility to extract native MVPN backup file from it. Backup manager backup file name has format***<MVPNGW01C<CLUSTERID>_<DEVICEID>_<TIMESTAMP>.zip.>***
   Native MVPN GW backup file name has format all-<TIMESTAMP>.tar.gz. For procedure **Recovering the Mobile VPN Gateway on page 167** use native MVPN GW backup file.
3. From the menu at the left, select **Schedule Backup**.
4. In the **Type** list, double-click **Moble VPN Gateway** item.
5. Execute Backup action.

   For each MVPN GW cluster the backup manager server has one registered application with ID in form **MVPNGW01Cxx** where **xx** is the Cluster ID (the value set during Configuring the Network Identity on page 65). Instances of Mobile VPN Gateway cluster have different configuration backup files and should be distinguished by a unique Cluster ID value.

5.2.2
Setting Backup Schedule for MPVN Gateway Cluster

Prerequisites:
Refer to *Enhanced Software Update* manual for instructions to obtain the MVPN Gateway backup file stored in the backup manager storage area. Backup files are used with Restoring the Mobile VPN Gateway on page 167 procedure.

When and where to use:
Perform this procedure to set the backup schedule for the MVPN gateway cluster. Backup and restore management feature supports two ways of performing backup:

Manual (on-demand) backup initiated by user with Backup role in backup manager console.

Scheduled backup initiated by backup manager server. By default MVPN Gateway registers schedule to perform backup once a day by 00:00 PM.

Procedure:

1. In a web browser recommended by the *Operations Support Platform Backup Manager Operator Guide*, open web address of backup manager server console.
2. Log on to backup manager server with the Backup role selected.
3. From the menu at the left, select **Schedule Backup**.
4. In the **Add Schedule service** section, specify the schedule parameters:

1. In the **Name** field, enter a name for the scheduled backup task.
2. Next to the **Agent** field, click **Select**.
3. In the **Choose agent** dialog box, select the entity for which you want to schedule a backup task, and click **Choose**.
   To ensure that only entities without scheduled backup tasks are displayed, you can check the **Not scheduled** checkbox.
4. From the **Recurrence** drop-down list, select either a daily or a weekly backup.
5. If you want to schedule a weekly backup, select a day to run the backup from the **Day** drop-down list.
6. From the **Hour** and **Minute** drop-down lists, select the specific time to run the backup.
7. If you want to schedule a daily backup, specify at what interval to run the backup by selecting a value from the **Interval** drop-down list.

5. Click **Submit** then **Activate** button.

   The MVPN Gateway backup will automatically perform according to the schedule.

5.3 Mobile VPN Gateway Statistics

The MVPN Gateway statistics functionality is installed with the initial installation, and is automatically enabled at startup. Statistic collection is continuously run while the system is up.

The statistics collected are:

- eth1 (average during an interval): in packets per second: kbytes per second, out packets per second, out kbytes per second
- eth2 (average during an interval): in packets per second: kbytes per second, out packets per second, out kbytes per second
- IPsec (at sample time): number of the established IKE subscriber accounts
- Other (at sample time): date/timestamp

Every 24 hours the current statistics file is compressed, archived, and stored at the same directory. The statistics are stored at the `/var/log/stats/` directory. Current statistics are located in the `vpn-stats.log` file. Archive retention is defaulted to 365 days, and is configured using the Statistics Administration submenu. Archive files older than the retention time span, are removed. The sample interval, or the frequency of sampling the statistical data, is defaulted to 60 seconds, and is also configured using the Statistics Administration submenus.

When configuring statistics, changes on one gateway virtual machine propagate to the all other virtual machines on the cluster. Changes take effect immediately on all virtual machines of the cluster. If one of the virtual machine gateways in the cluster is powered off, or otherwise inaccessible, the configuration fails and an error message is displayed. Changes are not applied. Correct the situation and re-enter the values desired.

NOTICE: If the total amount of IKE subscriber account sessions (all tunnels, currently raised to the VPN gateway) reaches 90% of that VPN capacity, according to the applied license, the statistics functionality sends a warning message to syslog in `/var/log/messages`.

5.3.1 Accessing the Statistics Administration Menu

Prerequisites: MVPN Gateway is functioning.

When and where to use: Access to configure or display MVPN statistics.

Procedure:

1. Log in to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **Statistics Administration**.

Postrequisites: Continue with Setting the Statistics Logging Configuration on page 129, Displaying the Statistics Logging Configuration on page 129, and Displaying Live Statistics on page 130 as needed.

5.3.2
Setting the Statistics Logging Configuration

Prerequisites: Perform Accessing the Statistics Administration Menu on page 128.

When and where to use: Configure the time periods for statistics monitoring (sample interval) and archive.

Procedure:

1. At the **Statistics Administration** menu, enter the number associated with **Set Statistics Logging Configuration**.
2. An interactive script runs. Enter the desired values.

   The range of the value and default values are shown with each prompt.

   Step example:

```
Enter selection (1-3,b,q): 2
Enter amount of days to keep statistic's logs: (1-365)[2]: 5
Enter sample interval (in seconds) for statistic's logs: (2-86400)[2]:
6
VPN statistic's daemon configuration was successfully added
```

5.3.3
Displaying the Statistics Logging Configuration

Prerequisites: Perform Accessing the Statistics Administration Menu on page 128.

When and where to use: Display the time periods for statistics monitoring (sample interval) and archive.

Procedure:

1. At the **Statistics Administration** menu, enter the number associated with **Display Statistics Logging Configuration**.
2. An output of the current statistics configuration displays.

   Step example:

```
The following values are currently configured:
  Days to Keep: 5
  Sample Interval: 6
```

5.3.4
Displaying Live Statistics

Prerequisites: Perform Accessing the Statistics Administration Menu on page 128.

When and where to use: Display the current (live) statistics.

Procedure:

1. At the **Statistics Administration** menu, enter the number associated with **Display Live Statistics**.
2. An output of the current statistics monitoring displays. The screen is refreshed every 2 seconds until the user presses Q to quit.

   Step example:

```
     : STAT        :        CURRENT :             AVG :             PEAK :
 ike : up          :              4 :            4.00 :                4 :
eth1 : rx_pps      :           0.00 :            0.00 :             0.00 :
eth1 : rx_kbps     :           0.00 :            0.00 :             0.00 :
eth1 : tx_pps      :           0.00 :            0.00 :             0.00 :
eth1 : tx_kbps     :           0.00 :            0.00 :             0.00 :
eth2 : rx_pps      :           0.00 :            0.14 :             1.00 :
eth2 : rx_kbps     :           0.00 :            0.32 :             2.22 :
eth2 : tx_pps      :           0.00 :            0.14 :             1.00 :
eth2 : tx_kbps     :           0.00 :            0.29 :             2.03 :

Press 'q' to quit
```

5.4
Software Upgrade

Mobile VPN Gateway product allows upgrading of existing user configuration to latest release.

NOTICE: Mobile VPN Gateway does not support transition of single cluster configuration to Geo-Redundant configuration (two clusters). Additional new cluster has to be installed and configured from scratch.

5.4.1
Full Upgrade to Latest Version of Mobile VPN Gateway on ESXI Machine

Prerequisites:

1. Perform necessary BIOS and ILO upgrade.
2. Perform necessary ESXI upgrade.
3. Prepare service PC laptop which will be used to run restore configuration script. Verify connectivity from it to ESXI server with MVPN Gateway software. Follow the procedure Restoring the Mobile VPN Gateway on page 167. When warning message is displayed, that all MVPN connections are about to be disconnected and services are not available during restore procedure, enter No to cancel with restore procedure.
4. Obtain default credentials for default root, clusync in MVPN GW. Verify credentials for existing root and hafence account in ESXI servers as they will be needed for deployment, cluster definition and restoration.
5. vSphere connectivity to both ESXI available with root account.
6. Perform test deployment of OVF image with new version of software to both ESXI. Use ***<testvm>*** name to deploy virtual machine and boot it. Verify there are no checksum and non-compatibility

warnings. Shutdown and remove test virtual machine after validation. It should be done after ESXI upgrade.

When and where to use: Use this procedure to configure Non-Redundant and Redundant configuration with no limit to service downtime.

Procedure:

1. Create backup file from installation of old version of the product. Follow the procedure Performing On Demand Backup for MVPN Gateway Cluster on page 126 for details. Verify downloaded backup file for ***<checksum>*** integrity.
2. Shutdown and remove virtual machines (old version of product) using vSphere client.
3. Deploy virtual machines (new version) for MVPN Gateway product. Same number and names of the vms are used as installation for the previous release. Follow the procedure Importing OVF into Virtual Server on page 55 for details.
4. Perform Configuring the Network Identity on page 65. The same agency and management network definitions are used in the installation for the previous release.
5. Perform the procedure Defining the Cluster on page 72.
6. Perform restoration of the configuration from backup file

5.4.2
Incremental Upgrade to Latest Version of Mobile VPN Gateway on ESXI Machine

Prerequisites:

- Prepare service PC laptop used to run restore configuration script. Verify connectivity from the PC laptop to the ESXI server with MVPN Gateway software, see Restoring the Mobile VPN Gateway on page 167. When warning message is displayed, that all MVPN connections are about to be disconnected and services are not available during restore procedure, enter **No** to cancel with restore procedure.
- Obtain default credentials for default root, clusync in MVPN GW. Verify credentials for existing root and hafence account in ESXI servers as they will be needed for deployment, cluster definition, and restoration.
- vSphere connectivity to both ESXI available with root account.

When and where to use:
Redundant configuration with minimal downtime impact required. Use this procedure to provide VPN service with virtual machines located on one ESXI in a redundant system, while performing upgrade tasks on another ESXI.

Procedure:

1. Create backup file from installation of the old version of the product. Follow the procedure Performing On Demand Backup for MVPN Gateway Cluster on page 126 for details. Verify downloaded backup file for ***<checksum>*** integrity.
2. Reinstall VPNGW virtual machines 2,4,6, and 8 hosted by ESXI 2:
   - Make VPN service inactive. Follow procedure 4.8.2 Setting the Mobile VPN Gateway Node Offline.
   - Shutdown and remove virtual machines (old version) of product using vSphere client.
   - Apply ILO, BIOS, and ESXI upgrades to physical server ESXI 2.

- Deploy virtual machines of new version of MVPN Gateway product. Same names of vms should be used as in installation for previous release, see Importing OVF into Virtual Server on page 55 for details.
- Perform Configuring the Network Identity on page 65. Same Agency and management network definitions should be used as in installation for previous release.

3 Reinstall VPNGW virtual machines 1,3,5, and 7 hosted by ESXI 1:

- Shutdown and remove virtual machines (old version) of product using vSphere client.
- Apply ILO, BIOS, and ESXI upgrades to physical server ESXI 1.
- Deploy virtual machines of new version of MVPN Gateway product. Same names of vms should be used as in installation for previous release. Follow the procedure Importing OVF into Virtual Server on page 55 for details.
- Perform Configuring the Network Identity on page 65. Same Agency and management network definitions should be used as in installation for previous release.

4 Perform Defining the Cluster on page 72.

5 Perform restoration of configuration from backup file.

Chapter 6

Mobile VPN Gateway Server Troubleshooting

6.1 Mobile VPN Gateway Connection Issues

The most common causes of Mobile VPN connection issues are listed in this section together with probable solutions.

Table 14: VPN Connection Issues

Problem	Cause	Solution
Secure tunnel is established but no traffic is passed.	Motorola Solutions Mobile VPN Gateway does not have the application network route configured.	Use the Routing Configuration menu option to add the correct routing table entry for the Internal Network Interface.
	Network cable is unplugged.	Check with the network administrator to ensure network is properly configured.
	Traffic is being blocked by an upstream firewall.	Check with the network administrator to ensure network is properly configured.
	Network VLAN IDs are misconfigured.	Check with the network administrator to ensure network is properly configured.
	Client address pool is not in the internal routing infrastructure routing table.	Check with the network administrator to ensure network is properly configured.
Secure tunnel traffic is experiencing poor performance or significant packet loss.	Mobile VPN gateway is overloaded.	Verify if the number of connected clients does not exceed the maximum.
Unable to connect to defined profile.	Wrong profile is selected.	Provide correct client ID (See Profile Differentiation on page 134.)
Unable to connect with Windows client.	Default Windows-specific algorithms are disabled.	Enable algorithms. (See Enabling Algorithms Used by Windows VPN Client on page 134.)
Client does not send certificate upon authentication.	Wrong date on device.	See Certificate Time Range Validity on page 138.
Unable to connect to VPN with certificate authentication using CRL.	Certificate is mistakenly generated with CRL.	See Certificate Verification with CRL on page 138.

Table continued…

Problem	Cause	Solution
Unable to connect to VPN with certificate authentication using CRL.	Certificate cannot be validated due to connection failure to the server providing the CRL file.	See Disabling of CRL Validation on page 139.

6.1.1
Profile Differentiation

By default, connection profiles have equal priority. If the wrong profile is selected, a VPN connection might not be established at all, or established with the wrong profile, hence providing undesired access or functionality to client. The only way to properly differentiate connection profiles is to provide the correct client ID (**rightid** parameter in access profile).

- The order of the values in the DN string is important:
  “CA Subject DN” value can contain wildcard * to match relative distinguished names (RDN). In order to match a wildcard template, the DN of a peer must contain the same number of RDNs, in exact order defined by the “CA Subject DN” template.
  The following RDNs are supported: DC, C, ST, L, O, OU, CN, ND, N, G, S, I, T, E, Email, emailAddress, SN, serialNumber, D, UID, ID, unstructuredName, UN, employeeNumber, EN. Example: In template "CN=*, OU=IPsec, OU=Public Safety, O=PKI, C=US" the RDN CN (Common Name) matches to any value.
- The value for **rightid** is the DN attribute of the client certificate which the client uses to authenticate itself. This can be found by enabling and checking the IPsec log file.

  See the following example of user the DN highlighted in the IPsec log.

```
02:07:16 20[ENC] parsed IKE_AUTH request 1 [ IDi N(INIT_CONTACT) SA AUTH
CERTREQ CERT CERT TSi TSr N(MOBIKE_SUP) ]
02:07:16 20[IKE] received cert request for "CN=System5RSATa01, OU=PKI,
O=pslte.msi.com, L=SCH, ST=IL, C=US"
02:07:16 20[IKE] received cert request for "CN=System5RSACa01, OU=PKI,
O=pslte.msi.com, L=SCH, ST=IL, C=US"
02:07:16 20[IKE] received end entity cert "CN=VML-CAI1554R4N,
O=pslte.msi.com, OU=IPsec, OU=sitetosite, L=SCH, ST=IL, C=US"
02:07:16 20[IKE] received issuer cert "CN=System5RSACa01, OU=PKI,
O=pslte.msi.com, L=SCH, ST=IL, C=US"
```

6.1.2
Enabling Algorithms Used by Windows VPN Client

By default these algorithms are disabled.

ESP:

aes256-sha1-modp1024

aes256-sha1

IKE:

aes256-sha384-prfsha384-modp1024

Algorithms are configurable in Strongswan Global Values, and synchronized among Service Groups. See Setting Global Parameters for Connection Profiles on page 109

6.1.3
Authentication for APX radios

IMPORTANT: Do not configure APX radios to use certificates. The Mobile VPN Gateway blocks any traffic from APX radios that are configured to use certificates.

6.1.4
IPsec and Firewall File Configuration

Each time the Administrator creates a connection profile and adds an authentication method, MVPN Gateway software automatically updates all necessary system configuration, as well as synchronizes it to the redundant server. Direct file changes in Strongswan configuration files or in iptables combined with using the administration menu to configure connection profiles are not supported and lead to failures in VPN functionality.

IMPORTANT: Do not modify your ipsec.conf or iptables manually.

6.2
Troubleshooting ESXi Server Issues

When and where to use:
One or more of the following conditions are noted:

- The user is not able to access the guest virtual machine (VM) console through the vSphere client. The console remains blank and displays the error message: `Unable to connect to the MKS: Connection terminated by server` or `Unable to connect to the MKS: Malformed response from server`.
- Log in to the ESXi server through SSH fails because the SSH connection session cannot be established.

Procedure:

1 Perform one of the following:

NOTICE: The recovery steps listed in the table may cause a temporary interruption in currently active sessions to the ESXi server. The user may need to log in through the vSphere client after this procedure.

If…	Then…
the ESXi server is not accessible through SSH,	Perform step 2 through step 6.
the ESXi server is accessible,	Perform step 7 through step 14.

2 Connect a monitor and keyboard directly to the HP DL380 server.

3 Press ALT+F1 and log in to ESXi as **root**

4 Change directories by entering: `cd /etc/init.d`

5 Restart all the ESXi management agents by entering: `services.sh restart`

6 Wait for the restart function to complete.

7 Connect to the ESXi server through SSH and log in as **root**

8 Change directories by entering: `cd /etc/init.d`

9 Restart the ESXi management agent by entering: `hp-ams.sh restart`

10 Attempt to access the guest VM console again.

11 If the issue persists, restart all the ESXi management agents by entering: `services.sh restart`

12 Wait for the restart function to complete.

13 After all the management agents are restarted, attempt to access the guest VM console again.

14 If the issue persists, power down all the virtual machines on the ESXi server. Reboot the ESXi server by entering: `reboot`

6.3 Recovering from a Missing VMDK File

When and where to use:
Use when a Virtual Machine (VM) fails to power on and the error message states that the VM's vmdk file was not found.

For example: `File []/pdr01.zone1_1.vmdk was not found`

In this case the (VMDK) descriptor file for the PDG VM was missing at the time of power on.

Procedure:

1 Log on as `root` into the terminal of the ESXi/ESX host using PuTTY.

2 To navigate to the directory that contains the virtual machine disk with the missing descriptor file, enter: `# cd /vmfs/volumes/`***`<datastore>`***`/`***`<virtual machine dir>`***

3 Identify the type of SCSI controller the virtual disk is using.

You can do this by examining the virtual machine configuration file (`.vmx`). The controller is identified by the line `scsi#.virtualDev`, where # is the controller number.

Step example:
With `pvscsi`

`cat`***`<virtual machine name>`***`.vmx | grep virtualDev`

pciBridge4.virtualDev = "pcieRootPort"

pciBridge5.virtualDev = "pcieRootPort"

pciBridge6.virtualDev = "pcieRootPort"

pciBridge7.virtualDev = "pcieRootPort"

scsi0.virtualDev = "pvscsi"

ethernet0.virtualDev = "vmxnet3"

ethernet1.virtualDev = "vmxnet3"

4 Identify and record the exact size of the `-flat` file which is missing the corresponding vmdk.

See the following example:

Step example:
`# ls -l `***`<vmname_diskno>`***`-flat.vmdk`

`-rw------- 1 root root`***`<size in bytes>`***`Oct 11 12:30 `***`<vmname_diskno>`***`-flat.vmdk`

5 Note down the ***`<size in bytes>`*** and use it in the next step.

6 To create a virtual disk, enter the vmkfstools command: `# vmkfstools -c `***`<size in bytes>`***`-a `***`<virtual_controller>`*** `-d thin temp.vmdk`

- The command uses the following flags: -c *size*

- The following is the size of the virtual disk:

  -a virtual_controller (As captured in step 3, for example: **pvscsi**)

- The following creates the disk in thin-provisioned format: -d thin

To save disk space, we create the disk in **thin-provisioned** format using the type **thin**. The resulting flat file then consumes minimal amounts of space (1 MB) instead of immediately assuming the capacity specified with the -c switch. The only consequence, however, is the descriptor file contains an extra line that must be manually removed in a later step.

You have successfully created the `temp.vmdk` and `temp-flat.vmdk` files.

7 To delete the `temp-flat.vmdk` file, enter: `# rm temp-flat.vmdk`

8 To rename the `temp.vmdk` file to the name required to match the orphaned **.flat** file, enter: `# mv temp.vmdk` ***<vmname_diskno>***`.vmdk`

<vmname_diskno>`.vmdk` corresponds to ***<vmname_diskno>***`-flat.vmdk`

9 Edit the new `vmdk` file using **vi**.

10 Under the **Extent Description** section, change the name of the `.flat` file to match the orphaned `.flat` file you have:

<vmname_diskno>`-flat.vmdk)`

11 Find and remove the line **ddb.thinProvisioned = "1"**

Step example: (only the sections bolded)

Disk DescriptorFile

version=1

CID=fb183c20

parentCID=ffffffff

createType="vmfs"

Extent description

RW 8388608 VMFS **"*<vmname_diskno>*-flat.vmdk"**

The Disk Data Base

#DDB

ddb.virtualHWVersion = "4"

ddb.geometry.cylinders = "522"

ddb.geometry.heads = "255"

ddb.geometry.sectors = "63"

ddb.adapterType = "lsilogic"

ddb.thinProvisioned = "1" (Remove Line)

The virtual machine is now ready to power on.

12 Verify your changes before starting the virtual machine.

13 To check the disk chain for consistency, run the following command against the disk descriptor file : `# vmkfstools -e` ***<vmname_diskno>***`.vmdk`

For a complete chain, you see output similar to: `Disk chain is consistent`

For a broken chain, you will see a summary of the snapshot chain and then an output similar to: `Disk chain is not consistent:` The parent virtual disk has been modified since the child was created. The content ID of the parent virtual disk does not match the corresponding parent content ID in the child (18).

6.4 Cleaning up VMware Child Processes

The issue is observed when an attempt is made to access a Virtual Machine console using the vSphere Client. The following error message appears: `VMRC console can't be connected`.

Procedure:

1. On the Windows where this issue is seen, launch the **Task Manager** by right-clicking on the **Taskbar** and selecting **Start Task Manager**.
2. Under the **Processes** tab, search for any `vmware-vmrc.exe` processes.
3. Select `vmware-vmrc.exe`.
4. Click **End Process**.
5. For all instances of `vmware-vmrc.exe` process, repeat step 2 and step 3.
6. Start the **vSphere Client**. Connect to the host directly or to vCenter Server and ensure that virtual machine console can be viewed.

6.5 Installation and Customization

If **custom management IP address** is selected, upon cluster definition, the administrator **must** select **CUSTOMIZE** and manually provide the management address IPs of all the MVPN GW servers.

The hostname prefix defined in set-identity must be the same across all MVPN Gateway servers in an MVPN cluster. MVPN Gateway server hostname must be identical to the ESXi VM name of the deployed MVPN Gateway server.

6.6 Certificate Management

6.6.1 Certificate Time Range Validity

A certificate is issued with a constraint which limits its validity to a specific time period. It is important to understand that the current time on the device or server is used when confirming certificate validity, which occurs before other verifications.

IMPORTANT: If local device time is misaligned (for example, Jan. 1, 1970) and certificate validity period starts since July 1, 2015, the certificate may be considered as invalid.

Make sure all devices maintain proper actual time, especially if they use certificates to authenticate.

6.6.2 Certificate Verification with CRL

- A CRL server (or many) must be accessible from VPN GW (routing).
- A CRL file can be cached, and may not be updated every time.
- It is possible to temporarily disable CRL verification.

If the CRL Enforcement Policy is configured as “no” and the CRL URI is present in the certificate, but points to an inaccessible location, then establishing the VPN tunnel takes longer than usual. (Additional time is needed for the CRL fetching timeout.)

For a basic explanation of certificates with the CRL feature, see Certificate Revocation List (CRL) on page 33.

A certificate revocation list (CRL) is a list of certificate identifiers (serial numbers) which have been revoked by the PKI administrator and should no longer be trusted. A revoked certificate can no longer be used for authentication purposes.

The PKI administrator has the option of creating a certificate by providing an address where the CRL file can be obtained.

When the client sends a certificate to authenticate itself with CRL specified, Strongswan VPN software checks whether the CRL file contains an indication that the certificate has been revoked. If the CRL file is missing from the local server cache or has expired, Strongswan VPN software will attempt to download this file from specified address of CRL. If the CRL address is not accessible and the file cannot be downloaded, the VPN connection will not be established.

IMPORTANT: A reliable link must be maintained between the MVPN Gateway and PKI server with the CRL. Additionally, ensure CRL files are accessible to download from the PKI server for further validation.

Routing must be configured to ensure the PKI server is reachable with the IP from the MVPN Gateway server.

The address of the CRL file can specified with different application protocols, such as HTTPS or LDAP. The administrator needs to determine which mechanism will be used for CRL delivery and ensure all intermediate firewalls will pass the TCP traffic required for transferring it.

In the case where the administrator knows there will be no access to CRL files located in the PKI server from the Gateway, certificates for devices must be generated without CRL.

WARNING: The policy of certificate-based authentication without CRL validation introduces risk of security violation and has to be carefully verified before its acceptance.

6.6.3
Disabling of CRL Validation

WARNING: Disabling CRL validation should be done in **emergency situations** only!

Symptoms:

1. The PKI server where CRL files are located is not accessible from the MVPN Gateway. This can be due maintenance or failure of server or network link.
2. Devices are provisioned with certificates having a CRL option.
3. The device attempts to connect to a protected network with the Gateway, but the authentication is rejected because the CRL file is missing in the local cache, or present but has expired.

To prevent service deniability of MVPN Gateway due to PKI issues, the dministrator can temporarily disable CRL validation on the MVPN Gateway server. That will allow authentication with VPN on all devices, including these whose certificate was blacklisted with CRL.

WARNING: All existing VPN connections will be discarded. This procedure should be applied to each server in the cluster.

How to Disable

Log in as **root** to GW server.

Run the following commands:

```
cd /usr/lib64/strongswan/plugins
mv libstrongswan-revocation.so libstrongswan-revocation.so-off
service strongswan restart
```

How to Enable

Run the following commands:

```
cd /usr/lib64/strongswan/plugins
mv libstrongswan-revocation.so-off libstrongswan-revocation.so
service strongswan restart
```

6.6.4

Certificate Chain Issues

To diagnose some issues with certificate file access and validation see Viewing Certificate Import Logs on page 143.

General requirement issues:

Certificate chain has only 1 certificate – a chain must contain at least root CA certificate and server certificate.

Certificate attributes are missing or incorrect. See Server Certificate Attributes on page 140.

Certificate chain must be imported to the same server where the CSR file comes from.

File layout issues:

Only `.crt` or `.pem` file extensions for certificate files are allowed.

Certificate files must have Unix line ending format.

Each certificate from the chain should reside in its own file.

No other files or folders should be present on CD/DVD media.

ESXi-related issues:

Only one CD/DVD image is mounted in ESXi with vSphere Client.

If mounted CD/DVD cannot be accessed by MPVN Gateway software, reboot of MVPN Gateway server is required.

6.6.5

Server Certificate Attributes

Example of a certificate for the MVPN Gateway server:

X509v3 Key Usage critical:
Digital Signature, Non Repudiation, Key Agreement
1.3.6.1.4.1.19718.1000.1.2.2:
1.3.6.1.4.1.19718.1000.1.2.3:
1.3.6.1.4.1.19718.1000.1.2.1:

X509v3 Extended Key Usage: TLS Web Server Authentication, IP security end entity
X509v3 Subject Alternative Name: DNS:system5vpngw7.pslte.msi.com, DNS:system5vpngw7, DNS:10.10.10.11
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.19718.1000.1.1.0.0
Policy: 1.3.6.1.4.1.19718.1000.1.1.1.1

X509v3 Subject Key Identifier: 70:B6:72:15:B0:80:7D:4B:CF:04:BF:DD:40:EC:A2:92:49:C5:4C:77
X509v3 Basic Constraints critical: CA:FALSE

X509v3 Authority Key Identifier: keyid:35:21:4D:88:74:6E:DF:5F:D9:AF:5F:EF:6D:77:56:83:16:B2:17:74

X509v3 CRL Distribution Points:

Full Name:

URI:ldap://10.10.10.12:49504/cn=System5ECC1Ca01,ou=CDP,o=pslte.msi.com,dc=System5CR01cr1?certificateRevocationList

6.7 Mobile VPN Gateway Logs

StrongSwan software can be configured for logging, in multiple levels of detail separately for each internal subsystem, for all Mobile VPN session establishment events, including failures. All logging and detail level is user configured. Logging can be configured to be local.

The logs are stored in the following locations:

- StrongSwan (IPsec gateway software) logs: `/var/log/charon.log`
- Cluster events: `/var/log/cluster/`
- System log (which may include a subset of the strongSwan or cluster logs/events): `/var/log/messages`

6.7.1 Managing IPsec Logging

IPsec (strongswan charon process) logging can be enabled and disabled by the Administrator from the Administration menu.

When and where to use:

NOTICE: Enabled IPsec logging is required by the log analyzer to discover certain issues related to certificate authentication.

CAUTION: Enabling logs impacts VPN performance negatively. It is recommended for short time diagnostics only.

Procedure:

1. Log in to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with `Application Administration`.
4. At the **Application Administration** menu, enter the number associated with `IPSec Log Settings`.
5. At the **IPsec Log Settings** menu, enter the number associated with `Enable logging`.

   This operation requires Administrator confirmation.
6. At the confirmation prompt, enter: `y`

6.7.2 Viewing IPsec Log File

Procedure:

1. Log in to the Mobile VPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with `OS Administration`.
4. At the **OS Administration** menu, enter the number associated with `Display Logs`.
5. At the **View Logs** menu, enter the number associated with `IPSec Log Files`.
6. At the **IPsec Log Files** menu, enter the number associated with `charon.log`.

6.7.3
IPsec Log Analyzer

Mobile VPN Administration Menu provides access to tool automatically inspecting IPsec log (`charon.log` file) for presence of several known types of problems, such as connection issues.

NOTICE: IPsec logging must be enabled in order to use automated inspection. The tool uses current IPsec `/var/log/charon.log` file. It should be taken into account that the content of this log file is archived once a day, and older log entries become unavailable for checking.

The tool is able to find out the following kinds of situations:

Error situation	Displayed message
Problem with Certificate Revocation List download.	Failed to fetch CRL from: `CRL_URI`. Verify connectivity.
Missing client certificate.	No certificate received from client, but needed. This might be a result of invalid date or time settings on the devices.
Remote Access profile matched when Site To Site client tried to connect.	Invalid connection profile matched. All certificate authentication methods for Site To Site and Remote Access profiles should have defined disjoint rightid to properly differentiate them.
Site To Site profile matched when Remote Access client tried to connect.	Invalid connection profile matched. All certificate authentication methods for Site To Site and Remote Access profiles should have defined disjoint rightid to properly differentiate them.

6.7.3.1
Using the Log Analyzer Tool

Prerequisites: See IPsec Log Analyzer on page 142.

Procedure:

1. Log in to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with `Application Administration`.
4. At the **Application Administration** menu, enter the number associated with `Perform Log Analyze`. Provide time window for log analyze.

Period must be shorter than 24h.

Step example: 2h30m

5 Provide the value of how long the oldest analyzed logs could be.

6 Wait for the result. Found errors with corresponding log fragments are displayed.

```
No certificate received from client, but needed. This might be a
result of invalid date or time settings on the devices.

17:13:58 74[NET] received packet: from 10.200.0.6[500] to
10.190.2.133[500] (456 bytes)
17:13:58 74[ENC] parsed IKE_AUTH request 1 [ IDi N(INIT_CONTACT) SA
AUTH
CERTREQ TSi TSr ]
17:13:58 74[IKE] received cert request for "CN=phase one ecc384 issuing
ca, OU=PKI, O=pkiphaseone.pslte.com, C=OM"
17:13:58 74[IKE] received cert request for "CN=phase one ecc384 root
ca,
OU=PKI, O=pkiphaseone.pslte.com, C=OM"
17:13:58 74[CFG] looking for peer configs matching
10.190.2.133[%any]...
10.200.0.6[CN=VML-351901060003070, OU=IPsec, OU=CAR,
O=pkiphaseone.pslte.com, C=OM]
17:13:58 74[CFG] selected peer config 'Site_to_Site-1-Auth-ECDSA1-
CERT0.crt'
17:13:58 74[IKE] no trusted ECDSA public key found for
'CN=VML-351901060003070, OU=IPsec, OU=CAR, O=pkiphaseone.pslte.com,
C=OM'
17:13:58 74[ENC] generating IKE_AUTH response 1 [ N(AUTH_FAILED) ]
17:13:58 74[NET] sending packet: from 10.190.2.133[500] to
10.200.0.6[500] (88 bytes)
```

6.8 Viewing Certificate Import Logs

Procedure:

1 Log in to the Mobile VPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `admin_menu`

3 At the **Main Menu**, enter the number associated with **OS Administration**.

4 At the **OS Administration** menu, enter the number associated with **Display Logs**.

5 At the **View Logs** menu, enter the number associated with **Certificate Import Log Files**.

6 At the **Certificate Import Log Files** menu, enter the number associated with **cert-admin.log**.

6.9 SNMP Fault Management

The Mobile VPN Gateway provides integration with the Unified Event Manager (UEM) server. The purpose of the UEM server application is to monitor the health of devices in the zone, such as servers, and zone controllers. The status information of a device is obtained using the Simple Network Management Protocol (SNMP).

6.9.1
Mobile VPN Gateway Managed Objects

The Mobile VPN Gateway provides integration with the Motorola Solutions Unified Event Manger (UEM) server to view managed objects and alarms. In the UEM, you can view three managed object events sent to the UEM:

- Application object
- Service Managed object
- Application Link Management object

These views and their operations are explained in detail in *Unified Event Manager* manual.

6.9.1.1
Mobile VPN Gateway Application Object

Application managed object (.1.3.6.1.4.1.161.3.6.82.2.1) represents the state of one Mobile VPN Gateway (MVPNGW) virtual server instance, as show in the following table.

Table 15: Application Object States

Value	Managed Resource	Description	Impact on IP-SEC Service Availability	Severity
1	EnabledActive	The MVPNGW server instance provides VPN service.	Up	Clear
2	EnabledStandby	The MVPNGW server instance is ready to provide VPN service.	Down	Clear
3	Disabled	The MVPNGW server instance is disabled.	Down	Warning
4	Malfunction	The MVPNGW server instance is in failure state.	Down	Critical

Table 16: Application Object State-Cause Mapping

Value	Valid States	Cause	Description	Planned
1	EnabledActive, EnabledStandby, Disabled	Normal	The MVPNGW server is enabled and fully operational as a result of either a normal initialization or user request.	true
2	Malfunction	GenericFailure	NVPNGW server is non-operational due software or configuration error.	false
3	Malfunction	FirewallFailure	MVPNGW server capabilities are affected due non-operational iptables.	false

Table continued…

Value	Valid States	Cause	Description	Planned
4	Malfunction	NoLicenseFailure	MVPNGW server capabilities are affected due lack of license.	false

6.9.1.2

VPN Service Managed Object

Mobile VPN Gateway Service object (.1.3.6.1.4.1.161.3.6.82.2.2) represents state of process responsible for IPsec capabilities to user as shown in the following table. This is associated with the High Availability feature controlling access to IPsec functionality in redundant and non-redundant installations.

Table 17: VPN Service Object States

Value	Name	Description	Impact on IPSEC Service Availability	Severity
1	Enabled	VPN service instance is active.	Up	Clear
2	EnabledHALost	VPN service instance is active but lost HA capability.	Up	Warning
3	Disabled	VPN service instance is inactive.	Down	Warning
4	Malfunction	VPN service instance is in failure state.	Down	Critical

Table 18: VPN Service Object State-Cause Mapping

Value	Valid States	Cause	Description	Planned
1	Normal, EnabledHALost,Disabled	Normal	Result of either a user action or normal initialization.	true
2	Malfunction	GenericFailure	Result of software or configuration failure.	false

6.9.1.3

Application Link Managed Object

Mobile VPN Gateway Service object (.1.3.6.1.4.1.161.3.6.82.2.3) represents the state of a network link as shown in the following table. Multiple link instances are included - Internal, External, Management, and High Availability.

Table 19: VPN Service Object States

Value	Name	Description	Impact on IP-SEC Service Availability	Severity
1	Up	Link is fully operational	Up	Clear
2	Down	Link is not operational.	Down	Critical

Table 20: Application Link Object State-Cause Mapping

Value	Valid States	Cause	Description	Planned
1	Up	Normal	Link performs correctly.	true
2	Down	GenericFailure	Link is absent, disabled, or malfunctioned.	false
3	Down	Unreachable	Remote destination is unreachable	false
4	Down	Authentication-Failure	Remote destination refuses communication due to authentication errors.	false

6.9.2

Mobile VPN Gateway Alarms

All alarms are associated with Mobile VPN Gateway (MVPNGW) Application managed object. An alarm results from an event in a managed resource. It occurs as a result of a pre-determined significant state (a failure or a fault) that may require user attention. Alarms are raised within the UEM based on notifications from the network element, or by the UEM to report failures associated with fault management functions. Alarm messages consist of short problem descriptions and possible resolution.

Table 21: VPN Service Object States

Alarm Code	Alarm Name / Text	Severity	When
1001	SysIpsecRestart	Critical	Triggers upon IPsec software restart

Table continued…

Alarm Code	Alarm Name / Text	Severity	When
Possible Resolutions - IPsec software has been forcibly restarted. Server restart is recommended for recurring incidents. If the problem persists after reboot, Contact Motorola Solutions technical support.			
1101	CfgSyncFailureOSPF	Warning	Triggers upon OSPF configuration replication error
Possible Resolutions - OSPF configuration replication error. Verify accessibility of all servers in service group with clusync user on Secure Shell (SSH) management interface. Repeat configuration change action to enforce data synchronization. If the problem persists, contact Motorola Solutions technical support.			
1102	CfgSyncFailureFirewallBypass	Warning	Triggers upon firewall bypass configuration replication error
Possible Resolutions - Firewall bypass rule configuration replication error. Verify accessibility of all servers in service group with clusync user on Secure Shell (SSH) management interface. Repeat configuration change action to enforce data synchronization. If the problem persists, contact Motorola Solutions technical support.			
1103	CfgSyncFailureVpnProfile	Warning	Triggers upon IPsec configuration replication error
Possible Resolutions - IPsec configuration replication error. Verify accessibility of all servers in service group with clusync user on SSH management interface. Repeat configuration change action to enforce data synchronization. If the problem persists, contact Motorola Solutions technical support.			
1201	BackupFailure	Critical	Triggers upon failure of backup operation.
Possible Resolutions - Backup operation failed. Verify accessibility of all servers in service group with clusync user on SSH management interface. If the problem persists, contact Motorola Solutions technical support.			
1202	RestoreFailure	Critical	Triggers upon restore operation failure.
Possible Resolutions - Restore operation failed. Verify accessibility of all servers in service group with clusync user on SSH management interface. If the problem persists, contact Motorola Solutions technical support.			
1301	VpnServerCertificateExpiring	Warning	Triggers once per 24 hours if server certificate is going to be expired in the next 30 or less days.
Possible Resolutions - The server certificate to expire soon. Install new server certificate chain in advance to ensure continuity of VPN client authentication process. If certificate validity period assumes its use in present time and beyond, verify local time on MVPNGW server.			
1302	VpnServerCertificateExpired	Warning	Triggers once per 24 hours if server certificate is expired.

Table continued…

Alarm Code	Alarm Name / Text	Severity	When
Possible Resolutions - Server certificate is expired. Remove existing expired server certificate. Install new server certificate chain to provide authentication of VPN clients. If certificate validity period assumes its use in present time and beyond, verify local time on MVPNGW server.			
1303	VpnServerCertificate-NotValidYet	Info	Triggers once per 24 hours if server certificate is not yet valid.
Possible Resolutions - Server certificate is not yet valid. Installed certificate chain is not yet valid to provide authentication of VPN clients. If certificate validity period assumes its use in present time and beyond, verify local time on MVPNGW server.			

6.10 OSPF Routing Issues

By default, all inbound OSPF routes are accepted from adjacent RED SWITCH router. Inbound OSPF routes configure same type of routes as mentioned in section Configuring VPN Internal Routing on page 81 but in an automated manner. If this behavior is not acceptable, the administrator can disable or filter certain OSPF routes from being applied to kernel routing.

6.10.1 Disabling Inbound OSPF Routing

When and where to use:
Only static VPN internal routing allowed. This procedure must be applied on each service group.

Procedure:

1. Log on to vpngw server as a root user.
2. From the command prompt, enter: `ospf-adm.pl --permit-inbound-routes=none`
3. The output messages display:

```
OSPF successfully configured
```

6.10.2 Filtering Selected Inbound OSPF Routing

When and where to use:
Mixed VPN internal and selected OSPF routing allowed. Procedure must be applied on each service group.

Procedure:

1. Log on to vpngw server as a root user.
2. From the command prompt, enter one of the following commands:

   ```
   ospf-adm.pl --permit-inbound-routes=CIDR
   ospf-adm.pl --permit-inbound-routes=CIDR-RANGE
   ```

   where:

   - CIDR - limit inbound OSPF routes with specific CIDR to apply to local machine routing. Example: the value 192.168.0.0/16 will enable only routes to 192.168.0.0 with mask length 16.

- CIDR-RANGE - limit inbound OSPF routes with specific CIDR range to apply to local machine routing. CIDR range has the format `'NETWORK/MIN-MASK le MAX-MASK'`. **Example:** The value "192.168.0.0/16 le 32" will enable all routes '192.168.?.? with mask length in range 16-32. A range includes routes like 192.168.0.0/16, 192.168.100.0/24 and 192.168.0.8/29

3 The output messages display:

```
OSPF successfully configured
```

6.10.3

Enabling Inbound OSPF Routing

When and where to use:
Use this procedure to restore default behavior. Procedure must be applied on each service group

Procedure:

1 Log on to vpngw server as a root user.

2 From the command prompt, enter: `ospf-adm.pl --permit-inbound-routes=all`

3 The output messages display:

```
OSPF successfully configured
```

This page intentionally left blank.

Chapter 7

Mobile VPN Gateway FRU/FRE Information

This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) for the Motorola Solutions Mobile VPN Gateway and includes references to replacement procedures for these items.

7.1 Mobile VPN Gateway Server FRU List

The following table lists the part numbers and references to the appropriate procedure for replacing the Motorola Solutions Mobile VPN Gateway server FRUs (Field Replaceable Units).

Table 22: Mobile VPN Gateway Server FRU List

Component Type	Part Number	Replacement Procedure
Hard Drives HP 1.2 TB 6G SAS 10K 2.5in SFF HDD	DLN6942A	For the appropriate replacement procedures, see the *HP ProLiant DL380 Gen9 Server User Guide*.
HP 800W Flex Slot Platinum Hot Plug Power Supply	DLN6864A	
HP 9.5MM SATA DVD-RW JACKBLACK GEN9 OPTICAL DRIVE	DLN6866A	

7.2 Mobile VPN Gateway Server FRE

The following table lists the part numbers and references to the appropriate procedure for replacing the Motorola Solutions Mobile VPN Gateway server FRE.(Field Replaceable Entity).

Table 23: Mobile VPN Gateway Server FRE

Component Type	Part Number	Replacement Procedure
Virtual Server HP DL380	DLN6943A	See the *HP ProLiant DL380 Gen9 Server User Guide*. Go to http://www.hp.com/go/docs and select Gen9 > DL380.

7.2.1

Hardware Component Configuration

For this release, the Mobile VPN Gateway HP DL380 Gen9 is configured as shown:

Table 24: HPDL380 Gen9 Configuration for the Mobile VPN Gateway

Component	Description
Processor	Two Intel® Xeon® E5-2680 v3 (2.50GHz/12-core/30MB/9,6GB/s QPI/120W)
System Memory	64GB Total (8 x 8GB 1Rx4 PC4-2133P-R Kit (DDR4-2133))
Hard Disk Controller	HP Smart Array P440ar/2GB FBWC (RAID 0/1/1 ADM/1+0/1+0 ADM/5/5+0/6/6+0)
Hard Drives	Two HDD - HP 1.2TB 6G SAS 10K 2.5in SFF SC DP ENT
Optical Storage Device	HP 9.5MM SATA DVD-RW JACKBLACK GEN9 OPTICAL DRIVE
Removable Storage	HP 8GB microSD EM Flash Media Kit
Network Interface Cards (NICs)	Four built-in NIC ports and 16 external NIC ports (4 x HP Ethernet 1Gb 4-port 331T Adapter)
Graphics Processor with Memory	Graphics Processor with Memory Integrated Matrox G200 video
Power Supplies	Two Power Supplies total (2 x HP 800W Flex Slot Platinum Hot Plug Power Supply Kit)

Chapter 8

Bare-Metal Setup of HP ProLiant DL380 Gen9 Servers

This chapter contains procedures for a bare-metal configuration of HP ProLiant DL380 Gen9 servers.

Bare-metal configuration is performed for a new installation, when the server is pre-loaded with RAID, BIOS, iLO firmware, and VMware ESXi at the factory. Follow instructions in this process to check and skip or perform the pre-loaded steps.

8.1 Setting Up the Hardware Platform for the Mobile VPN Gateway Server

This process describes the configuration of HP ProLiant DL380 Gen9 Unified Extensible Firmware Interface (UEFI), the installation and licensing of the VMware ESXi hypervisor on the Mobile VPN Gateway Server, and several other configuration tasks.

Prerequisites:
Ensure that VMWare ESXi installation media is available.

When and where to use: Perform this process if the VMware ESXi hypervisor has not been installed on the Mobile VPN Gateway server at the factory. For example, during a drop ship hardware installation or a field re-scratch if the previous installations have been corrupted.

Process:

1. Prepare installation environment for the Mobile VPN Server:
   - **a** Install the Microsoft .NET Framework on a client computer or technician service laptop.
     See Installing the .NET Framework on page 154.
   - **b** Install the Windows Management Framework.
     See Installing the Windows Management Framework on page 154.
   - **c** Install the VMware PowerCLI and PuTTY.
     See Installing VMware PowerCLI and PuTTY on page 155.
   - **d** Install the VMware vSphere Client on Windows-based devices.
     See Installing the VMware vSphere Client on Windows-Based Computer on page 158.
2. Set up the hardware for the Gen9 server:
   - **a** Update Gen9 BIOS and iLO Firmware.
     See Updating HP DL380 Gen9 BIOS and iLO Firmware on page 159.
   - **b** Set up initial iLO access on the Mobile VPN Server.
     See Setting up Initial Access to iLO on page 160.
   - **c** Enable FIPS mode for the iLO on the DL380 servers.
     See Enabling FIPS Mode on the iLO on page 161.
   - **d** Configure DL380 Gen9 iLO settings.
     See Configuring DL380 Gen9 iLO Settings on page 162.

e Configure Gen9 BIOS.

See Configuring HP DL380 Gen9 BIOS on page 164.

f Configure the HP ProLiant DL380 Gen9 UEFI settings.

See Configuring HP ProLiant DL380 Gen9 UEFI on page 164.

g Set up RAID for Gen9.

See Setting Up RAID for Gen9 on page 165.

3 **For redundant configuration:** repeat "Step 2".

8.1.1

Mobile VPN Gateway Installation Environment Preparation

Perform procedures in this section only once on a technician PC with Windows to prepare the installation environment.

8.1.1.1

Installing the .NET Framework

Prerequisites:
Obtain the *VMware vSphere Configuration Media*.

When and where to use:
Perform this procedure on a client computer or technician service laptop for the initial installation of Mobile VPN Gateway, and for performing backup and recovery operations on the Mobile VPN Gateway cluster.

Procedure:

1 Into the optical drive of the client computer or technician service laptop, insert the *VMware vSphere Configuration Media*.

2 Using Windows Explorer, navigate to the `Microsoft .NET Framework` directory on the *VMware vSphere Configuration Media*.

Step example: If your optical drive letter is `E:\`, navigate to `E:\Microsoft .NET Framework`.

3 Launch `NDP452-KB2901907-x86-x64-AllOS-ENU.exe`.

4 In the **.NET Framework Setup** window, select the **I have read and accept the license terms.** check box.

5 Click **Install**.

6 When the installation is complete, click**Finish**.

8.1.1.2

Installing the Windows Management Framework

The Windows Management Framework includes updates to Windows PowerShell. PowerShell 4.0 is required to install and configure the Dot Hill AssuredSAN 4524 Direct-Attached Storage array using a dedicated PowerShell script. PowerShell 4.0 is required for the execution of the PowerShell script, as well as for the subsequent network configuration.

Prerequisites:
Obtain the *VMware vSphere Configuration Media*.

Close all **PowerShell** windows.

When and where to use:
Perform this procedure on a client computer or technician service laptop for the initial installation of MVPN Gateway, and for performing backup and recovery operations on MVPN Gateway cluster.

Procedure:

1. Into the optical drive of the Windows-based device, insert the *VMware vSphere Configuration Media*.
2. Using Windows Explorer, navigate to the `Microsoft Windows Management Framework` directory on the *VMware vSphere Configuration Media*.

   Step example: If your optical drive letter is `E:\`, navigate to `E:\Microsoft Windows Management Framework`.
3. Launch `Windows6.1-KB2819745-x64-MultiPkg.msu`.
4. Follow the on-screen instructions to complete the installation.

8.1.1.3
Installing VMware PowerCLI and PuTTY

Prerequisites:
Obtain:

- Administrator credentials for the Windows-based computer where you will install VMware PowerCLI and PuTTY
- VMware vSphere Configuration Media

Procedure:

1. Click the **Start menu** and navigate to **All Programs** → **VMware**.
2. Perform one of the following actions:

If…	Then…
If the vSphere VMware PowerCLI menu exists and has contents,	perform an upgrade, see Upgrading VMware PowerCLI and PuTTY on page 157.
If the vSphere VMware PowerCLI menu does not exist,	continue with the next step.

3. Insert the **VMware vSphere Configuration Media** into the drive of the computer where the vSphere client resides.
4. Navigate to the **VMware vSphere PowerCLI** folder.
5. Locate and double-click **VMware-PowerCLI.exe** to launch the program.
6. If a pop-window appears, click **Continue** or **Yes**.

   The **VMware PowerCLI Installation Requirements** window appears.
7. Click **Install**.

   The **VMware Remote Console Plug-in Installation Welcome** window appears.
8. Click **Next**.

   The **Ready to Install VMware Remote Console Plug-in Components** window appears.
9. Click **Install**.

   The program is installed. The **Installation Wizard Completed** window appears.

10 Click **Finish**.

The **VMware VIX Installation Welcome** window appears.

11 Click **Next**.

The **VMware VIX License Agreement** window appears.

12 Select **I accept the terms in the license agreement**.

13 Click **Next**.

The **Destination Folder** window appears.

14 Click **Next**.

The **Ready to Install the Program** window appears.

15 Click **Install**.

The program is installed. The **Installer Completed** window appears.

16 Click **Finish**.

17 Optional: If a pop-up window appears, click **Continue**.

The **VMware Power CLI Installation Welcome** window appears.

18 In the **Welcome to the InstallShield Wizard** window, click **Next**.

19 Select **I accept the terms in the license agreement**.

20 Click **Next**.

The **Custom Setup** window appears.

21 Click **Next**.

The **Ready to Install the Program** window appears.

22 Click **Install**.

The program is installed. The **InstallShield Wizard Completed** window appears.

23 Click **Finish**.

24 Optional: Create a short cut of PowerCLI on the desktop.

a Click the **Start menu** and navigate to **All Programs** → **VMware** → **VMware vSphere PowerCLI**

b Right click the **powerCLI** item and drag it to the desktop

25 Open the **Start** menu.

26 Type `command` in the **Search programs and files** text field.

27 Right-click **Command Prompt** in the search results, and select **Run as administrator**.

The **Command Prompt** window opens.

28 At the command prompt, enter `powershell`

29 At the PowerShell prompt, enter `set-executionpolicy remotesigned`.

The access policy for PowerShell is modified.

30 At the PowerShell prompt, enter `new-eventlog application -source esxiconfig`

An event source for ESXi is created.

31 Close the command prompt window.

32 Install PuTTY on the computer where the vSphere client resides.

The PuTTY executable can be loaded to the local Windows machine from the **VMware vSphere Configuration Media**.

8.1.1.3.1

Upgrading VMware PowerCLI and PuTTY

Prerequisites:
Obtain:

- Administrator credentials for the Windows-based computer where you will install VMware PowerCLI and PuTTY
- *VMware vSphere Configuration Media*

Procedure:

1. Insert the *VMware vSphere Configuration Media* into the drive of the computer where the vSphere client resides.
2. Navigate to the **VMware vSphere PowerCLI** folder.
3. Locate and double-click `VMware-PowerCLI.exe` to launch the program.
4. If a pop-up window appears, click **Continue** or **Yes**.

   A prompt appears stating that an upgrade of PowerCLI is performed.
5. Click **Yes**.

   The VMware PowerCLI installation requirements window appears.
6. Click **Install**.

   The **VMware Remote Console Plug-in Installation Welcome** window appears.
7. Click **Next**.

   The **Ready to Install VMware Remote Console Plug-in Components** window appears.
8. Click **Install**.

   The program is installed. The **Installation Wizard Completed** window appears.
9. Click **Finish**.

   The user is prompted to uninstall the previous version of VMware VIX.
10. Click **OK**.

    The **VMware VIX Installation Welcome** window appears.
11. Click **Next**.

    The **VMware VIX License Agreement** window appears.
12. Select **I accept the terms in the license agreement**.
13. Click **Next**.

    The **Destination Folder** window appears.
14. Click **Next**.

    The **Ready to Install the Program** window appears.
15. Click **Install**.

    The program is installed. The **Installer Completed** window appears.
16. Click **Finish**.

    The **VMware Power CLI Installation Welcome** window appears.
17. Click **Next**.

The program is installed. The **Install Shield Wizard Complete** window appears.

18 Click **Finish**.

NOTICE: At this point, the upgrade for power CLI is complete. If there is an error or the upgrade fails, repeat this procedure by right-clicking **VMware-PowerCLI.exe** and selecting **Run as Administrator**, and continue from step 3.

19 Optional: Create a shortcut for PowerCLI on the desktop.

a From **Start**, navigate to **All Programs** → **VMware** → **VMware vSphere PowerCLI**

b Right-click the **powerCLI** item and drag it to the desktop.

20 Open the **Start** menu.

21 Type `command` in the **Search programs and files** text field.

22 Right-click **Command Prompt** in the search results, and select **Run as administrator**.

The **Command Prompt** window opens.

23 At the command prompt, enter: `powershell`

24 At the PowerShell prompt, enter: `set-executionpolicy remotesigned`.

The access policy for PowerShell is modified.

25 At the PowerShell prompt, enter: `new-eventlog application -source esxiconfig`

An event source for ESXi is created.

26 Close the command prompt window.

27 Optional: Install PuTTY on the computer where the vSphere client resides.

The PuTTY executable can be loaded to the local Windows machine from the **VMware vSphere Configuration Media**.

8.1.1.4

Installing the VMware vSphere Client on Windows-Based Computer

The VMware vSphere Client provides a graphical user interface for managing the ESXi server and virtual machines on the ESXi server. It also provides access for interacting with the virtual machines.

This procedure installs and upgrades the existing version of the vSphere client on the Windows-based device.

Prerequisites:

- The ESXi OS has been successfully installed and configured on the HP DL380 server.
- You have located the *VMware vSphere Configuration Media* that shipped with this release; the disc contains the vSphere Client installation file.
- You have ensured there is a connection between the box where you are going to install the vSphere client and the ESXi/vCenter.
- You have closed any existing vSphere client instances which are currently open.

IMPORTANT: The vSphere Client and the ESXi host server are designed to work together. A mismatch of the related releases causes unexpected results.

When and where to use:
Install the current release of the VMware vSphere Client.

NOTICE: Also see Logging On to the VMware vSphere Client on page 53.

Perform this procedure to install VMware vSphere client software.

Procedure:

1. Insert the *VMware vSphere Configuration Media* disc into the optical drive of the Windows-based local machine.
2. On the *VMware vSphere Configuration Media* disc, navigate to the `VMware vSphere Client` folder.
3. Launch `VMware-viclient-all.exe`.
   - If a message appears instructing you to install Microsoft®.NET Framework, click **OK**.
   - If a pop-up warning you about the PowerShell execution policy of the computer not being set to “RemoteSigned” appears, click **Continue**.
4. In the language selection window, select **English (United States)**. Click **OK**.
5. Follow the on-screen instructions to complete the installation.

   NOTICE: If the installation fails due to the previous version of vSphere Client being installed and the following message appears: `Failed to install hcmon`, please follow the steps below prior to continuing the installation:

   1. On the Windows desktop, right-click the **Computer** icon and select **Manage**.
   2. In the **Computer Management** window, click **Device Manager**.
   3. From the top menu bar in the **Device Manager** window, select **View** → **Show hidden devices**.
   4. In the list of device categories, double-click **Non-Plug and Play Drivers**.
   5. Right-click **VMware hcmon** and click **Uninstall**.
   6. Navigate to the `C:\windows\system32\drivers\` folder and rename `hcmon.sys` to `hcmon.sys.old`
   7. Repeat this procedure as a user with administrator privileges.

8.1.2
Hardware Setup for Gen9 Server

Perform procedures in this section to set up the Gen9 server.

8.1.2.1
Updating HP DL380 Gen9 BIOS and iLO Firmware

Prerequisites:
Connect a monitor, a keyboard, and a mouse to the server that you are upgrading.

Procedure:

1. Reboot or power on the server.
2. Eject the optical drive and insert the HP Firmware installation media into the optical drive. Close the drive tray.
3. At the prompt, select **Boot Menu** by pressing F11.
4. At the prompt, from the **One-time Boot Menu**, select the option corresponding to **ILO Virtual**.
5. Within 30 seconds of the prompt appearing, select **Interactive Firmware Update** by using the arrow keys. Press ENTER.
6. Select the **English** check box.

7 Accept the license by selecting the **Accept** check box. Click **Next**.

8 Click **Firmware Update**. Wait for the HP Smart Update Manager screen to load.

9 At the **Localhost Guided Update – Step 1 – Inventory of baseline and node** window, wait for the **Inventory of baseline** and **Inventory of localhost** progress bars to complete. Click **Next**.

10 At the **Localhost Guided Update – Step 2 – Review** window, leave the default selection of the components. Perform one of the following actions:

If…	Then…
If the Deploy button is enabled and the firmware versions on the server are older than the versions on the CD,	In the **Localhost Guided Update – Step 3 – Deployment** window, ensure that all components finished successfully. Click **Reboot**.
If the Deploy button is not enabled and the firmware versions on the server are newer than the versions on the CD,	perform the following actions: **a** Click **Back**. **b** Reboot the server by clicking the Power button icon.

11 At the confirmation prompt, click **Yes, reboot**.

12 Eject the optical drive and remove the installation media.

8.1.2.2

Setting up Initial Access to iLO

Integrated Lights Out (iLO) is an HP server management technology which allows monitoring and controlling of HP servers remotely. iLO allows you to connect to a server with a web browser on a computer or laptop, and perform configuration or maintenance activities. HP DL380 servers have a dedicated Ethernet port for iLO. This procedure sets up the network interface for the Integrated Lights Out (iLO).

Prerequisites:

- Ensure that the *System IP Plan* is available.
- Obtain the appropriate IP configuration from the *System IP Plan*.
- Obtain the default password from your system administrator.

Procedure:

1 Connect to the server through the serial connection through the terminal server.

2 Power on or reboot the server.

3 During the boot process, press F9 when prompted.

4 On the **System Utilities** screen, select **System Configuration** by using the arrow keys. Press ENTER.

5 On the **System Configuration** screen, select **iLO 4 Configuration Utility**. Press ENTER.

6 Optional: If prompted, provide Administrator login and password.

7 Select **Network Options**. Press ENTER.

8 Configure the iLO network options:

NOTICE: The iLO IP address and Gateway IP address should be taken from your IP Plan.

a Select **IP Address** and enter ***<Agency network prefix [a.b.c]>.<xyz>***

where:

<Agency network prefix [a.b.c]> is the first three octets, which are part of IP planning and commissioning data

<a>, ***<b>***, and ***<c>*** variables are numbers between 0–255, as defined in the *System IP Plan*

<xyx> is `143` for the physical GW1 server and `145` for the physical GW2 server (redundant only)

b Select **Subnet Mask** and enter `255.255.255.128`.

c Select **Gateway IP Address** and enter ***<Agency network prefix [a.b.c]>.<xyz>***

where:

<Agency network prefix [a.b.c]> is the first three octets, which are part of IP planning and commissioning data

<a>, ***<b>***, and ***<c>*** variables are numbers between 0–255, as defined in the *System IP Plan*

<xyx> is the Gateway IP address as stated in the *System IP Plan*

d Save your changes by pressing F10.

9 Exit the iLO 4 setup utility by selecting **File** → **Exit**. When prompted to confirm, press ENTER.

8.1.2.3
Enabling FIPS Mode on the iLO

Before configuring the iLO with custom user and licensing data, enable Federal Information Processing Standard (FIPS) mode on the Mobile VPN Gateway Server.

WARNING: Enabling FIPS mode restores the iLO to default factory settings and clears all user and license data, apart from the iLO IP configuration. If you enable FIPS mode after the iLO is configured with custom user and licensing data, all data except for the iLO IP configuration must be reapplied.

Prerequisites:
Set up iLO on the Mobile VPN Gateway Server. Obtain the default or customer-defined iLO username and password for the Mobile VPN Gateway Server. Obtain the *System IP Plan*.

Procedure:

1 To enable the FIPS mode for the iLO on the Mobile VPN Gateway Server, in a web browser, enter:
`https://`***<Agency network prefix [a.b.c]>.<iLO IP address>***

where:

<Agency network prefix [a.b.c]> is the first three octets, which are part of IP planning and commissioning data

<a>, ***<b>***, and ***<c>*** are numbers between 0–255

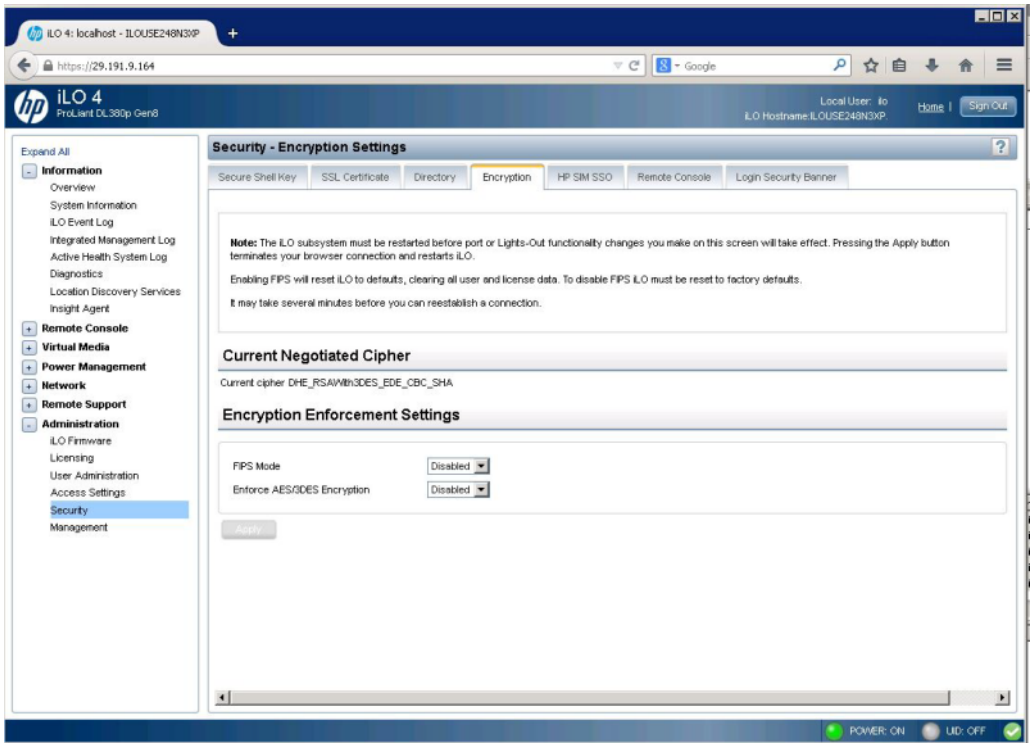
<iLO IP address> is the iLO IP address of your MVPN server, as stated in the *System IP Plan*

2 Log on to the iLO management page with the default or customer-defined username and password.

3 From the expandable menu on the left-hand side, select **Administration** → **Security**.

4 On the **Security — Encryption Settings** page, select the **Encryption** tab.

Figure 17: The Security — Encryption Settings Page on the iLO



5 In the **Encryption Enforcement Settings** pane, from the **FIPS Mode** drop-down menu, select **Enabled**. Click **Apply**.

Your browser session terminates and the iLO reboots.

8.1.2.4
Configuring DL380 Gen9 iLO Settings

Prerequisites:

1 Obtain the *VMware vSphere Configuration Media*.

2 Obtain the *System IP Plan*.

3 Prepare the Windows device with installed PowerShell software that can reach DL380 Gen9 through the network. See:

1 Installing the .NET Framework on page 154

2 Installing the Windows Management Framework on page 154

3 Installing VMware PowerCLI and PuTTY on page 155

4 Run the following commands in PowerShell in Administrator mode:

```
set-executionpolicy remotesigned
new-eventlog Application -Source esxiconfig
```

Procedure:

1 Insert the *VMware vSphere Configuration Media* into the optical drive of a Windows device that can reach the DL380 Gen9 through the network.

2 From **Start**, run the PowerShell command prompt as administrator:

a In the **Search programs and files** field, enter: `command`.

b In the search results, right-click **Command Prompt**, and select **Run as administrator**.

c At the command prompt, enter: `powershell`.

3 At the powershell prompt, enter the drive letter of the optical drive that contains the *VMware vSphere Configuration Media* followed by a colon.

Step example: `E:`

4 At the powershell prompt, enter: `cd common\bin`.

5 At the powershell prompt, enter: `.\Configure-ILOSettings.ps1`.

6 At the **Identity Type** prompt, enter: `2`.

7 At the **iLO IP Address** prompt, enter: ***<iLO IP address>***.

8 At the **iLO User Login Name** prompt, enter: `Administrator`.

9 At the **Password** prompt, enter the ***<iLO Administrator password>***.

10 At the **iLO Host Name** prompt, enter the ***<iLO Hostname>*** matching the IP plan value for this server.

11 At the **iLO Domain Name** prompt, enter the ***<iLO Domainname>*** matching the IP plan value for this server.

12 At the **iLO Subnet Mask** prompt, enter the ***<iLO Subnet Mask>*** matching the IP plan value for this server.

13 At the **iLO Gateway IP** prompt, enter the ***<iLO Gateway IP>*** matching the IP plan value for this server.

14 Perform one of the following actions:

- At the **DNS IP Address(es)** prompt, enter the ***<DNS IP Address(es)>*** matching the IP plan value for this server.
- If there is no DNS server in the system, do not enter a value.

15 Perform one of the following actions:

- At the **NTP Server IP Address(es)** prompt, enter the ***<NTP IP Address(es)>*** matching the IP plan value for this server.
- If there is no NTP server in the system, do not enter a value.

16 Perform one of the following actions:

- At the **Syslog IP** prompt, enter the ***<Syslog IP Address(es)>*** matching the IP plan value for this server.
- If there is no Syslog server in the system, do not enter a value.

17 At the **Time Zone** prompt, press ENTER.

18 At the **RIBCL File Path** prompt, press ENTER.

19 Enter: `y`.

20 If no errors appear in the output on the screen, press ENTER.

21 Enter: `exit` twice.

22 In a web browser on the PC or laptop, connect to `https://`***<iLO IP address>***.

23 Log on as Administrator.

24 In the left pane, expand the **Network** node and select **iLO Dedicated Network Port**.

25 In the right pane, select the **SNTP** tab.

26 From the **Time Zone** drop-down menu, select the appropriate time zone. Click **Submit**.

27 In the right pane, click **Reset**. Click **OK**.

Postrequisites: The iLO session is terminated. The process is complete.

8.1.2.5
Configuring HP DL380 Gen9 BIOS

Perform the following steps to configure BIOS on the HP DL380 Gen9 server.

Prerequisites:
Prepare the Windows device with installed PowerShell software that can reach DL380 Gen9 through the network. See:

1 Installing the .NET Framework on page 154
2 Installing the Windows Management Framework on page 154
3 Installing VMware PowerCLI and PuTTY on page 155

Procedure:

1 Insert the *VMware vSphere Configuration Media* into the optical drive of the Windows device connected to the server.
2 Select **Start** → **All Programs** → **Accessories** → **Windows PowerShell**, right-click the **Windows PowerShell** icon, and select **Run as administrator**.

   This step provides information on how to access Windows PowerShell on Windows 7. If you are using another version of Windows, the step may differ.
3 Enter the following commands:
   a Enter: `set-executionpolicy remotesigned`
   b At the prompt, enter: `y`
   c Enter: `new-eventlog Application -Source esxiconfig`
4 Enter the letter of the drive that contains the *VMware vSphere Configuration Media* followed by a colon.

   Step example: `E:`
5 Enter: `cd common\bin`
6 Enter: `.\Configure-BiosSettings.ps1`
7 At the **Identity Type** prompt, enter: `2`
8 At the **iLO IP Address** prompt, enter the iLO IP address.
9 At the **iLO User Login Name** prompt, enter: `Administrator`
10 Enter the iLO password for the `Administrator` user.
11 At the **BIOS JSON File Path** prompt, press ENTER.
12 Enter: `y`
13 Ensure that no errors appear in the output on the screen. Press ENTER.
14 To exit the PowerShell console, enter: `exit`

8.1.2.6
Configuring HP ProLiant DL380 Gen9 UEFI

This procedure describes the configuration of the HP ProLiant DL380 Gen9 Unified Extensible Firmware Interface (UEFI) using the BIOS/Platform Configuration (RBSU) menu.

When and where to use: Perform this procedure to configure Mobile VPN Gateway Server settings during a drop ship hardware installation.

Procedure:

1. Power on the server. At the **HP ProLiant** power-on self-test (POST) screen, press F9.

   To select menu options, use the arrow keys. Confirm all selections and changes to configuration settings by pressing ENTER.
2. At the **System Utilities** screen, select **System Configuration → BIOS/Platform Configuration (RBSU)**.
3. Select **Date and Time**. Configure the date and time:
   a. Select **Date (mm-dd-yyyy)** a enter the current date in the month-day-year format.
   b. Select **Time (hh:mm:ss)** and enter the current time in the 24–hour clock format.
   c. Select **Time Zone** and select your current time zone.
4. Return to the **BIOS/Platform Configuration (RBSU)** screen by pressing ESC.
5. Save your changes by pressing F10. At the `Changes are pending. Do you want to save changes and exit?` prompt, press Y.
6. At the prompt to select a reboot option, select **Reboot**.

8.1.2.7
Setting Up RAID for Gen9

Prerequisites:

1. Connect a USB keyboard, USB mouse, and VGA monitor to the DL380 Gen9.
2. Connect the power cords to the servers' power supplies.
3. Insert the local hard drives one at a time into the hard drive slots on the front of the DL380 chassis, starting at the left and moving right.
4. Plug the power cords into the power source; this will apply power to the server.

Procedure:

1. Boot the server.
2. When prompted during the boot process, press F10 to access the **Intelligent Provisioning** tool.
3. If prompted, select the license agreement check box. Click the right arrow button.
4. If a window appears asking to either activate or not activate the F10 option going forward, select the option associated with activation and click the right arrow to continue.
5. Click the **Register later** radio button. Click the right arrow to continue.
6. Click the **Perform Maintenance** icon.
7. After the **Intelligent Provisioning** tool launches, click the **HP Smart Storage Administrator (SSA)** option.
8. In the left pane, click **Smart Array P440ar**.
9. Click **Configure**.
10. Click **Create Array**.
11. Select the **Select All** check box.
12. Click **Create Array**.
13. Set the RAID level option to: **RAID 1**.

14 Click **Create Logical Drive**.

15 Click **Finish**.

16 Close the screen.

17 At the confirmation prompt, click **OK**.

18 Click the power symbol button at the top right of the screen.

19 Click **Reboot**.

Chapter 9

Mobile VPN Gateway Server Disaster Recovery

9.1 Recovering the Mobile VPN Gateway

Prerequisites:

- The procedure, Manually Backing Up all Mobile Virtual Private Network Gateway Cluster Configuration on page 125 has been performed.
- Backup files are available, depending on the condition of the MVPN hardware, either from the MVPN `/var/opt/perstore/restore/` directory, Backup and Restore Manager repository or from archived secure media (secure USB or CD/DVD).

NOTICE: If the backup files are unavailable, the MVPN Gateway can only be recovered as a new installation (no customer or custom configuration data are restored).

NOTICE: If one of the virtual machine gateways in the cluster is powered off, or otherwise inaccessible, the restore fails and an error message is displayed. Changes are not applied. Correct the situation and repeat this procedure. A warning message is sent to syslog in `/var/log/messages`

IMPORTANT: Results of the procedure, Joining the Mobile VPN Gateway to an Existing Domain Controller on page 67 are **not** part of the MVPN backup. After the MVPN system is restored from backup, perform the procedure again.

Process:

Contact your Motorola service representative about replacement hardware specifications. Perform one of the following:

If…	Then…
the replacement hardware does not have factory-installed software, RAID, BIOS, ESXi,,	Perform the procedures as a replacement installation. **a** See Installing and Configuring the Mobile VPN Gateway Servers on page 39 for optional steps for factory-installed software. **b** Perform the procedures in Restoring the Mobile VPN Gateway on page 167.
the replacement hardware does have factory-installed software, RAID, BIOS, ESXi,	Perform the procedures in Restoring the Mobile VPN Gateway on page 167.

9.2 Restoring the Mobile VPN Gateway

Restore the Motorola Solutions Mobile VPN Gateway from a replacement server.

Prerequisites:

- Installation procedures have been performed, see Installing and Configuring the Mobile VPN Gateway Servers on page 39.
- Obtain the back up (archive) media. See Manually Backing Up all Mobile Virtual Private Network Gateway Cluster Configuration on page 125.
- Obtain the *VMware vSphere Configuration Media*.

Procedure:

1. Log in to the MVPN Gateway (**vpngw1**). See Logging on to the Mobile VPN Gateway on page 111.
2. Copy the desired archive from the backup media to the `/var/opt/perstore/restore` directory.

   NOTICE: If Backup and Restore Manager integration is enabled and Backup and Restore Manager repository contains an archive copy of MVPN backup, restore the desired archive file from Backup and Restore Manager backup repository using Restore operation.
3. Insert the *VMware vSphere Configuration Media* disc into the optical drive of the Windows-based local machine.
4. On the *VMware vSphere Configuration Media* disc, navigate to the VMware vSphere Client folder.
5. On the Windows machine Client, right-click the **PowerCLI** shortcut and select **Run As System Administrator**.
6. At the PowerCLI console, run the MVPN Restore Cluster script by typing the following two commands:
   - `cd` ***`<VMware vSphere Configuration Media location>`***`\common\bin\`
   - `.\Restore-VPN-Cluster.ps1`
7. At the “Enter Primary ESXI IP:” enter the host IP from your customer-specific IP plan.
8. At the “Enter Primary ESXI username:” enter the administrative user name
9. At the “Enter Primary ESXI password:” enter the administrative user name password.
10. At the “Enter VPN gateway prefix:” enter the VPN gateway prefix (same as was specified during the set-identity procedure). See Configuring the Network Identity on page 65.
11. At the ***`<name of the vpngw1>`*** `username:` enter `root`
12. At the ***`<name of the vpngw1>`*** `password:` enter the root password.
13. The default selection for a single archive is automatic. If there are more than one archive in `/var/opt/perstore/restore`, a prompt is displayed to select the archive desired to restore the MVPN cluster.
14. A warning message is displayed, that all MVPN connections are about to be disconnected and services are not available during restore procedure.. Enter `Yes` to continue with restore procedure.
15. If the restoring cluster configuration is redundant, step 7 through step 9 are repeated for the secondary ESXI server (as the primary and secondary ESXi server).Continue with the next step.
16. If prompted for credentials for other gateways, enter the root credentials.
17. Wait for restore to complete (this can take up to 30 minutes). A success message is displayed:

    ```
    Restore-VPN-Cluster.ps1 run status [OK]
    ```
18. Press ENTER to exit.

19 Close the PowerCLI window.

The cluster is restored with the backup archive configuration. The strongSwan services are available.

9.2.1

Displaying Error Logging

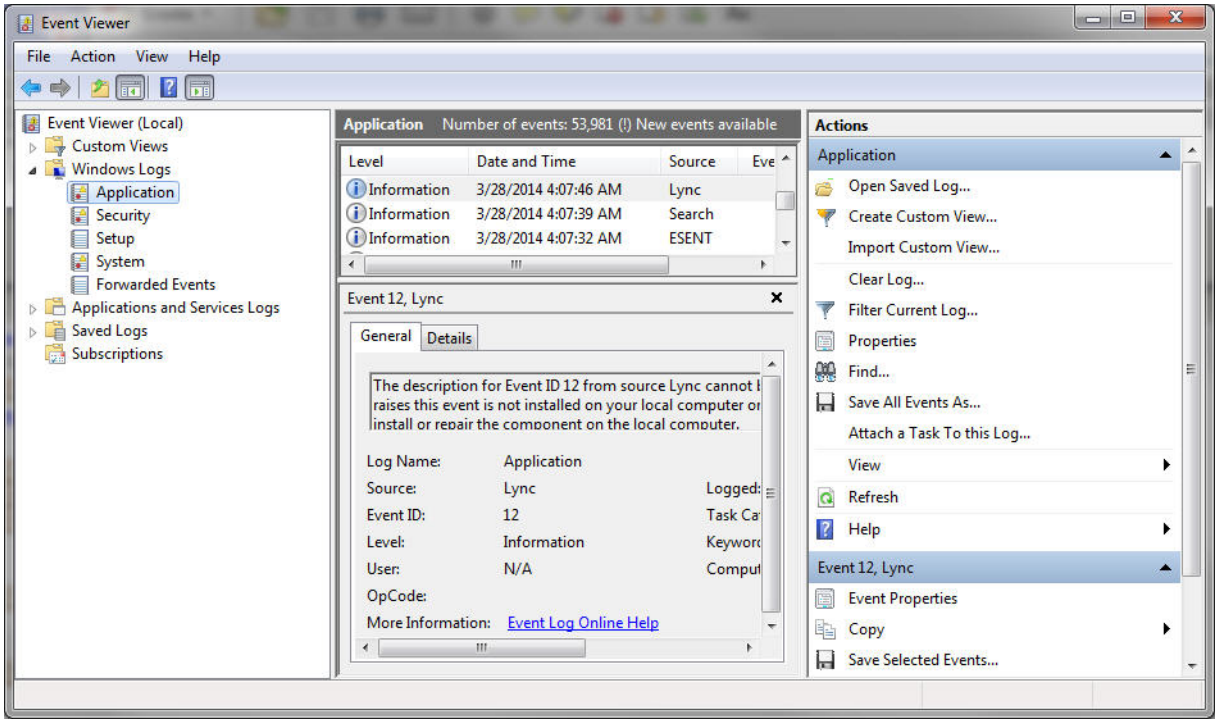
Prerequisites: A recovery has been performed. See Restoring the Mobile VPN Gateway on page 167.

When and where to use: Observe error logs after a recovery.

Procedure:

1. Select **Start**. Type **Event Viewer** at the search prompt.
2. Press ENTER to display the **Event Viewer**.

   Figure 18: Windows Event Viewer



3. In the left panel of the **Event Viewer** window, select **Windows Logs** → **Application**.
4. In the right panel of the **Event Viewer** window, click `Filter Current Log`.
5. In the pop-up **Filter Current Log**, select `esxiconfig` and `RestoreMVPN` options from the Event Sources drop down menu by selecting the check mark box next to the entries.
6. Click **OK**.

   Errors and information are listed in the middle panel for any needed analysis.

This page intentionally left blank.

Appendix A

Configuring User Equipment for Motorola Solutions VPN Service

The following list provides examples of procedures for configuring User Equipment for Motorola Solutions Mobile VPN service:

- For Windows clients (technician computers and/or end user mobile workstations), see:
  - Creating Motorola Solutions VPN Connection Profile in Windows on page 173
  - Configuring Motorola Solutions VPN Profile on Windows on page 174
  - Validating Motorola Solutions VPN Connection Profile in Windows on page 176

  Microsoft Windows 7, 8, and 8.1 can be installed on the Mobile VPN Gateway Server to support the Mobile VPN Gateway client.
- For importing certificates, see Importing Trust Chain Certificates on Mobile Workstations on page 171.
- See “Certificate” and “Setting the VPN” sections in the Public Safety LTE *VML750 Vehicular Subscriber Modem (VSM) Configuration Guide*.
- For instructions on using Motorola Solutions Radio Manager and Device Management Solution for configuring VPN and other applications on multiple devices simultaneously, see the Service Provisioning Guides for your specific model of Motorola Solutions mission critical handheld device (LEX series).
- For non-Motorola devices, see Accessing and Configuring Motorola Solutions VPN on Non-Motorola Devices on page 180.

A.1 Importing Trust Chain Certificates on Mobile Workstations

This procedure is performed by technicians who set up Windows-based computers to be clients of the Motorola Solutions Mobile VPN Gateway. This procedure imports the signed certificate and trust chain files provided by server administrators as described in the prerequisites.

Prerequisites:
Ensure that the Mobile VPN Gateway administrator completed Installing and Configuring the Mobile VPN Gateway Servers on page 39.

For mobile workstations:

- If certificates are used for the mobile workstation VPN client to authenticate to the Mobile VPN Gateway, obtain from the Mobile VPN Gateway administrator the signed certificate and trust chain files that match files imported to the Mobile VPN Gateway. Ensure that the administrator gives you the “Issued To” (Mobile VPN Gateway) name and “Issued From” (Trust Anchor/Certificate Authority) name so that you can verify after importing these files.
- Transfer these files to the mobile workstation. The local path and file names are required to complete this procedure. See the provisioning instructions for the device.

For Android devices:

- If certificates are used when Android users authenticate with Active Directory, obtain from the Active Directory administrator the signed certificate and trust chain files from Active Directory. Ensure that the administrator gives you the “Issued To” (Active Directory) name and “Issued From” (Trust

Anchor/Certificate Authority) name so that you can verify t after importing these files. The “Issued To” information for these files should be a name related to Active Directory such as Network Policy Server (NPS).

- Transfer these files to your Android device. The local path and file names are required to complete this procedure.

Procedure:

1. Log in to the Windows-based computer.

   Examples include, but not limited to, a user device, a server, or a laptop.

2. At the **Start** menu, type `mmc` in the search box.
3. Select `mmc.exe` from the results.

   The **Microsoft Management Console (Console 1)** window displays.

4. Select **File** → **Add/Remove Snap-in**.
5. Select **Certificates**.
6. Click **Add**.
7. In the pop-up window, select **Computer Account**.
8. Click **Next**.
9. Select **Local computer**.
10. Click **Finish**.
11. Click **OK**.
12. In the left pane, select **Certificates** → **Trusted Root Certification Authorities** → **Certificates**.
13. Right-click the **Certificates** folder, and select **All Tasks** → **Import**.

    The Certificate Import Wizard window displays.

14. Click **Next**.
15. Select **Browse**.

    The **Open file** window displays.

16. (Recommended): Select **All Files (*.*)** from the drop-down menu on the far right side of the window, to ensure that the required certificate files display in the next step.
17. Select the first certificate file saved to the mobile workstation, as described in the Prerequisites of this procedure.
18. Click **Next**.
19. Select **Place all certificates in the following store**.
20. Click **Next**.
21. Click **Finish** and wait for “The import was successful” message before proceeding to the next step.
22. Click **OK**.

    The **Microsoft Management Console (Console 1)** window displays.

23. Verify that the “Issued By” and “Issued To” information for the certificate file you imported appears in the list under **Certificates** → **Trusted Root Certification Authorities** → **Certificates** in the **Microsoft Management Console (Console 1)** window.

24 Repeat steps 13 through 22 for the remaining certificate and trust chain files that were saved to the mobile workstation, as described in the Prerequisites of this procedure.

25 Close the **Microsoft Management Console** window.

26 At the **Save console settings to Console 1?** pop-up window, click **No**.

A.2 Creating Motorola Solutions VPN Connection Profile in Windows

This procedure is performed by technicians who set up Windows computers to be clients of the Motorola Solutions Mobile VPN Gateway.

Prerequisites:
Ensure that the Mobile VPN Gateway administrator completed. See Installing and Configuring the Mobile VPN Gateway Servers on page 39.

From the Mobile VPN Gateway administrator, obtain the ***<IP address>*** for the Mobile VPN Gateway that should be used in this procedure.

From the Active Directory administrator, obtain the ***<user name>*** and ***<password>*** set up for this mobile workstation user in the “vpnusers” group.

Procedure:

1 Depending on your Windows OS version, perform one of the following actions:
- **For Windows 7**, from **Start**, select **Control Panel**.
- **For Windows 8 or 8.1**, from **Search**, open **Control Panel**.

2 In the **Search Control Panel** field, type in `vpn`.

3 Click **Set up a virtual private network (VPN) connection**.

4 Depending on your Windows OS version, perform one of the following actions:

If…	Then…
If your Windows version is Windows 7,	**a** In the **Create a VPN connection** window, select the **Don’t connect now; just set it up so I can connect later** check box. **b** In the **Create a VPN Connection** window, **Internet address** field, type in the ***<IP address>*** obtained from the Mobile VPN Gateway administrator. Click **Next**. **c** In the **User Name** and **Password** fields, type in the ***<user name>*** and ***<password>*** that were set up for this mobile workstation user in the “vpnusers” group by the Active Directory administrator. **d** If you want to remember your password, select the **Remember this password** check box.
If your Windows version is Windows 8 or 8.1,	**a** In the **Connect to a Workplace** window, select **I’ll set up an Internet connection later**. **b** In the **Connect to a Workplace** window, **Internet address** and **Destination name** fields, type in the ***<IP address>*** obtained from the Mobile VPN Gateway administrator and ***<user name>*** set up for this mobile workstation user in the “vpnusers” group by the Active Directory administrator.

If…	Then…
	Ignore the pop-up menu on the right.

5 Click **Create**.

Postrequisites: Proceed to Configuring Motorola Solutions VPN Profile on Windows on page 174.

A.3
Configuring Motorola Solutions VPN Profile on Windows

Perform this procedure to set up a connection profile that accommodates the necessary non-Suite B algorithms. Motorola Solutions Mobile VPN Gateway supports these non-Suite B algorithms for Windows, because the native Windows client does not fully support Suite B requirements.

Prerequisites:

- Obtain from your system administrator the host name of the Active Directory server that authenticates this Windows user.
- Perform Importing Trust Chain Certificates on Mobile Workstations on page 171.

Procedure:

1 Depending on your Windows OS version, perform one of the following actions:

If…	Then…
If your Windows version is Windows 7,	**a** From **Start**, select **Control Panel**. **b** In the **Search Control Panel** field, type in `network connection`. **c** Select **View network connections**.
If your Windows version is Windows 8 or 8.1,	**a** Open **Search**. **b** Type in `network connection` and, from the results, select **View Network Connections**.

2 In the **Network Connections** window, right-click the Motorola Solutions VPN connection profile that you created in Creating Motorola Solutions VPN Connection Profile in Windows on page 173, and select **Properties**.

3 Depending on your Windows OS version, perform one of the following actions:

If…	Then…
If your Windows version is Windows 7,	in the **VPN Connection Properties** window, select the **Options** tab and configure the following: **a** In the **Dialing options** section, confirm the **Display progress while connecting** and **Prompt for name and password, certificate, etc.** check boxes are selected. **b** In the **Redialing options** section, configure the fields per your system requirements.
If your Windows version is Windows 8 or 8.1,	continue with step 4.

4 Select the **Security** tab and configure the following:

a In the **Type of VPN** field, select **IKEv2** from the drop-down menu.

b In the **Data Encryption** field, select **Maximum strength encryption (disconnect if server declines)** from the drop-down menu.

c In the **Authentication** field:

1 Confirm the **Use Extensible Authentication Protocol (EAP)** check box is selected.

2 From the drop-down menu, select **Microsoft Protected EAP (PEAP) (encryption enabled)**.

3 Click **Properties**.

5 In the **Protected EAP Properties** window, **When connecting** section, configure the following:

a **For Windows 7:** Confirm the **Validate server certificate** and **Connect to these servers** check boxes are selected.

b **For Windows 8 or 8.1:** Select the **Verify the server's identity by validating the certificate** check box.

c Type in the ***<Active Directory hostname>*** in the **Connect to these servers** field.

d In the **Trusted Root Certification Authorities** section, select the "Issue From" certificate obtained from your administrator and installed on the mobile workstation.

See Importing Trust Chain Certificates on Mobile Workstations on page 171.

6 In the **Protected EAP Properties** window, **Select Authentication Method** section, configure the following:

a From the drop-down menu, select **Secured password (EAP-MSCHAP v2)**.

b Confirm **Enable Fast Reconnect** check box is selected.

7 Click **OK**.

8 Select the **Networking** tab and, in the **This connection uses the following items** list, configure the following:

a Clear the **Internet Protocol Version 6 (TCP/IPv6)** check box.

b Select the **Internet Protocol Version 4 (TCP/Pv4)** check box.

c Confirm **File and Printer Sharing for Microsoft Networks** and **Client for Microsoft Networks** check boxes are selected.

d Click **Properties**.

9 In the **Internet Protocol Version 4 (TCP/IP4) Properties** window, **General** tab, configure the following:

a Confirm **Obtain an IP address automatically** and **Obtain DNS server address automatically** check boxes are selected.

b Click **Advanced**.

10 In the **Advanced TCP/IP Settings** window, select the **IP Settings** tab and confirm the **Use default gateway on remote network** check box is not selected and the **Automatic metric** check box is selected.

11 Click **OK** three times to return to the **Network Connections** window.

The **Connecting to VPN Connection** window opens.

NOTICE: You may opt to start the VPN connection at this time or later. See Validating Motorola Solutions VPN Connection Profile in Windows on page 176.

12 To add the route for the gateway, run **Command Prompt** as Administrator.

The **Run Command Prompt as Admin** window opens.

13 In the `C:\Windows\system32>` prompt, type `"route print"`

An example of an `Interface List` displays. All numbers and names used in this procedure are for example purposes only.

```
===========================================================
  Interface List
25.........................VPN Connection
16...00 0c 29 8c c5 d1 ......Intel(R) PRO/1000 MT Network Connection #3
11...00 0c 29 8c c5 bd ......Intel(R) PRO/1000 MT Network Connection
 1...........................Software Loopback Interface 1
12...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
14...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
15...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
19...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #5
===========================================================
```

14 As the administrator, issue the command: `"route add <DEST> mask <Mask> 0.0.0.0 IF <VPN interface number> –p"`.

Step Example:
If protected network is: `192.163.1.0/24` and the VPN interface number is 25, then the command looks like: `route add 192.163.1.0 mask 255.255.255.255 0.0.0.0. if 25 –p`

NOTICE: To automatically add this route upon detection of network connection events add `"-p"` to the issue command.

15 Type `exit` to log out.

Postrequisites: To validate the configuration of the Motorola Solutions VPN Connection, perform Validating Motorola Solutions VPN Connection Profile in Windows on page 176.

A.4 Validating Motorola Solutions VPN Connection Profile in Windows

Perform this procedure to validate the Motorola Solutions VPN Connection on a Windows mobile workstation.

Procedure:

Depending on your Windows OS version, perform one of the following actions:

If…	Then…
If your Windows version is Windows 7,	**a** From **Control Panel**, select **Network and Internet**, then **Network Connections**. **b** Right-click the VPN connection that you want to validate and select **Connect**. **c** At the **Connect VPN Connection** window, provide the required Active Directory credentials: **a** ***<User name>*** **b** ***<Password>*** **c** ***<Domain>*** **d** Click **Connect**.

If…	Then…
If your Windows version is Windows 8 or 8.1,	**a** Open **Search**. **b** Type in `connect to a network` and, from the results, click **Connect to a network**. **c** From the list of available connections, select the connection and click **Connect**. **d** In the pop-up menu on the right, in the **Sign-in** area, type in the ***<Username>*** and ***<Password>*** that was set up for the mobile workstation the connection of which you want to verify. **e** Click **OK**.

After the information you supply is verified, the connection is completed.

This page intentionally left blank.

Appendix B

Motorola Solutions Mobile VPN Client Configuration on Android Devices

This chapter provides instructions for installation and configuration of the Motorola Solutions Mobile Virtual Private Network (VPN) client for non-Motorola devices.

NOTICE: For instructions on updating and configuring the Motorola Solutions Mobile VPN client on Motorola mission critical Android devices, see the staging/provisioning documentation for the specific device.

B.1
Assumptions and Prerequisites

Assumptions and prerequisites for installing and configuring the Motorola Solutions Mobile VPN client:

- Your organization implemented the Motorola Solutions Mobile VPN Gateway as its MVPN server.
- The Motorola Radio Management (RM) client and OMA-DM client are not available on your device.
- The Motorola Solutions Mobile VPN Gateway is installed in the agency-level network infrastructure and the **Remote Access** connection profile is created or configured. See Mobile VPN Gateway Installation on page 39 and Mobile VPN Gateway Configuration on page 61.
- The RSA/ECC key pair and signed certificate for the Android device are available.
- This installation sequence does not include items that are only available for Motorola devices, such as:
  - Steps for CRYPTR micro cards
  - Motorola OMA-based Device Management Solution (DMS) client installation
  - Radio Manager (RM) client installation

B.2
Motorola Solutions Mobile VPN Solution for Android Devices

Motorola Solutions Mobile VPN provides end-to-end data security between the end-user device and the customer's network, supporting device to agency confidentiality for all communications. This solution is designed to solve customers' security, connectivity, and mobility requirements.

Key differentiating features:

- Standards-based solution. Motorola Solutions Mobile VPN is built on IPsec and MOBIKE open standards.
- Supports end-to-end encryption.
- Supports Mobility and Application/Session Persistence.
- Supports enablement of mission critical data by supporting QoS and Priority, as outlined in standards (DSCP (ToS bits) Promotion).
- Supports standards-based authentication.
- Supports VPN and Mobile VPN Offering.
- Provides full redundancy support and solution is highly scalable which can be expanded and upgraded to fit user's needs (number of users, and so on).

Motorola Solutions Mobile VPN on Motorola devices (LEX 755, LEX L10, and so forth) offers more differentiating features like high assurance supports, client pre-loaded on devices (reduce installation costs).

The Android operating systems supported by the Motorola Solutions Mobile VPN client are:

- Android 4.2 and later.
- Software upgrades for Motorola Solutions Mobile VPN are provided through the Google Play store by updating manually or automatically.

B.3 Installing Motorola Solutions Mobile VPN on Non-Motorola Devices

Prerequisites: The Motorola Solutions Mobile VPN Gateway is installed in the agency-level network infrastructure.

When and where to use: Use this procedure to install the Motorola Solutions Mobile VPN client on non-Motorola devices in a public safety network that includes the Motorola Solutions Mobile VPN Gateway.

Procedure:

1. To install the Motorola Solutions Mobile VPN client on the device, perform one of the following actions:
   - Select **Mobile VPN** at www.motorolasolutions.com/mysoftware/apps, then use the **Download Now** button that displays.
   - Search for **Motorola Solutions Mobile VPN** in Google Play store and follow the instructions to download the application to your Android device.
   - From your e-mail account on your Android device, click the URL in the e-mail from your Motorola account representative to download the application to your Android device.
2. Perform Accessing and Configuring Motorola Solutions VPN on Non-Motorola Devices on page 180.

B.4 Accessing and Configuring Motorola Solutions VPN on Non-Motorola Devices

Use this procedure to configure the Motorola Solutions Mobile VPN client on non-Motorola devices in a public safety network that includes the Motorola Solutions Mobile VPN Gateway.

Prerequisites: The Motorola Solutions Mobile VPN client is installed on your non-Motorola device, see Installing Motorola Solutions Mobile VPN on Non-Motorola Devices on page 180.

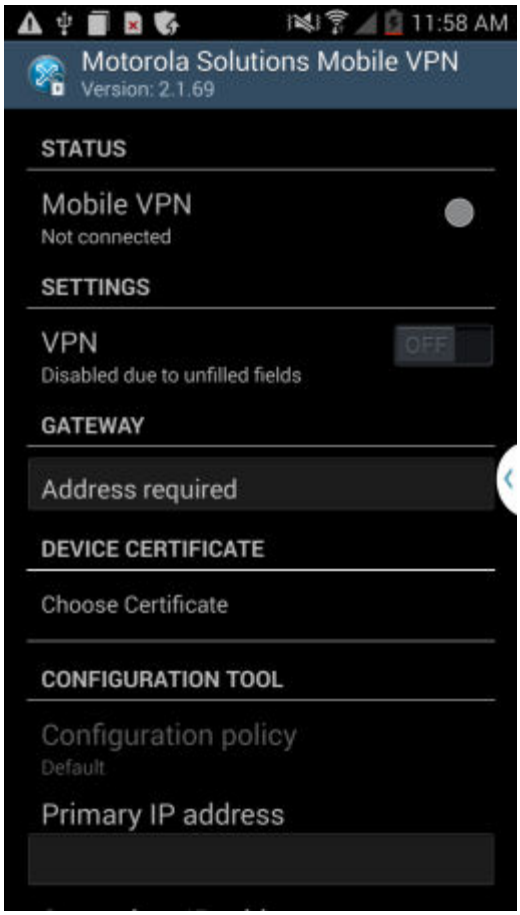
Procedure:

1. On the android device home screen, tap the **Motorola Solutions Mobile VPN** icon.

   The **Motorola Solutions Mobile VPN** screen displays.

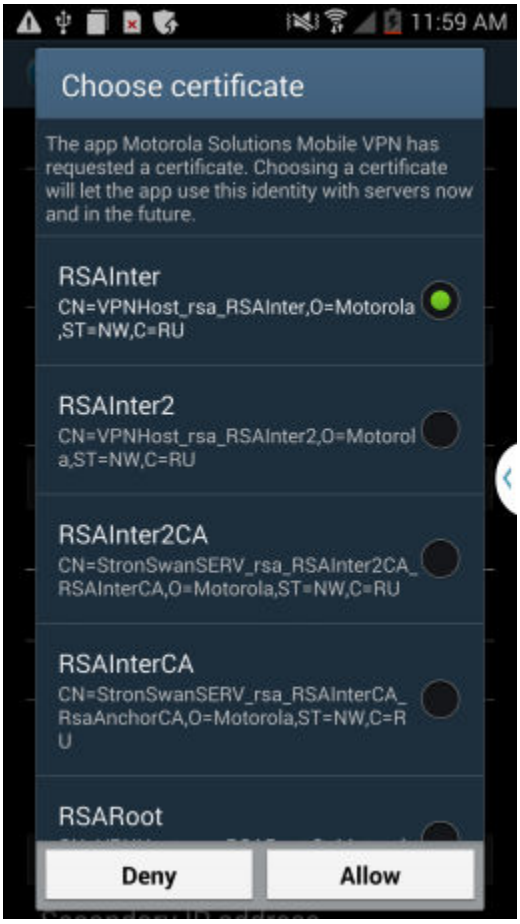
Figure 19: Motorola Solutions Mobile VPN Disabled



NOTICE: If the **CONFIGURATION TOOL** is available in your MVPN Client version, leave the default settings.

2 In the **DEVICE CERTIFICATE** section, tap **Manage certificate**.

Figure 20: Motorola Solutions Mobile VPN Choose Certificate



a From the **Choose Certificate** field, select a certificate, and tap **Allow**.

NOTICE: If installing a `.p12` certificate for the Motorola Solutions Mobile VPN, there is an extra **Install** instance on the Android device. Choose one of the following:

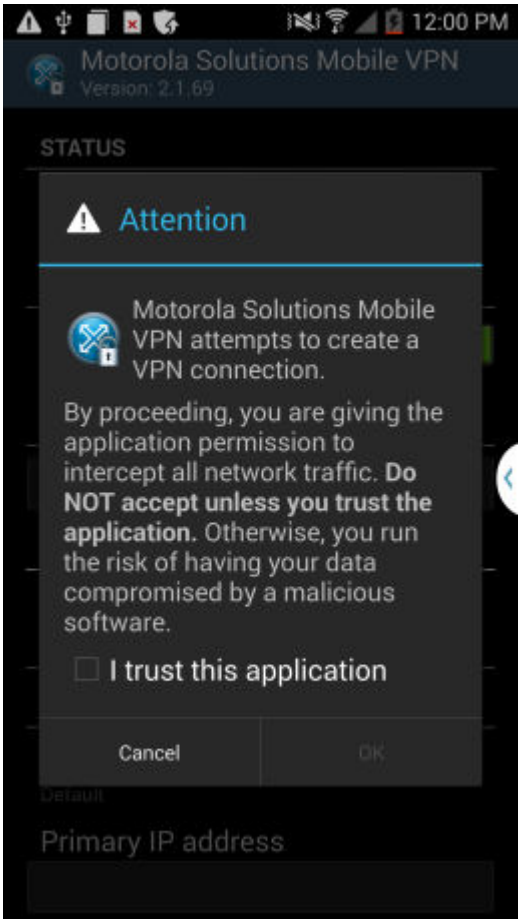
- **Select an existing certificate** and tap **Allow**, or
- Tap the extra **Install** button to install a new certificate.

3 In the **GATEWAY** field, confirm the IP address from your system IP Plan is entered.

4 In the **Motorola Solutions Mobile VPN** screen, from the **VPN** field, confirm the toggle is set to **ON**.

5 If the **Attention** screen appears, check **I trust this application** and tap **OK**.

Figure 21: Allow Motorola Solutions Mobile VPN



NOTICE: The **Allow Motorola Solutions Mobile VPN** screen appears when the Motorola Solutions Mobile VPN client is launched for the first time or VPN rights are revoked from Motorola Solutions Mobile VPN by another VPN solution (such as the default Android VPN). Give the Motorola Solutions Mobile VPN the required permission to access the VPN functions of your Android device.

6 Perform Verifying Connection Through the Motorola Solutions Mobile VPN Client User Interface on page 183.

Postrequisites: Contact your Motorola Solutions service representative, for coordination and transferring certificate requests and the resulting certificate files with a designated, trusted Certificate Authority. Transfer the CSR media to the certificate authority to generate and export signed certificates to secure media (CD/DVD) for importing to the Mobile VPN Gateway, see Importing Trust Chain Certificates on Mobile Workstations on page 171.

B.5 Verifying Connection Through the Motorola Solutions Mobile VPN Client User Interface

Perform the following procedure to verify that the connection through the Motorola Solutions Mobile VPN client was configured correctly.

Procedure:

1 On the home screen of your device, tap the **Motorola Solutions Mobile VPN** icon.

The **Motorola Solutions Mobile VPN** window displays.

Figure 22: Motorola Solutions Mobile VPN Enabled

2 From the **Motorola Solutions Mobile VPN** window, verify the following:

a In the **STATUS** section, confirm the **Mobile VPN** dot displays green.

b In the **GATEWAY** section, confirm the IP address from your system IP Plan displays.

c In the **DEVICE CERTIFICATE** section, confirm a certificate set displays.

d If the **CONFIGURATION TOOL** is available in your MVPN Client version, leave the default settings.

B.6

Troubleshooting for Motorola Solutions Mobile VPN Client

This section provides troubleshooting information for Motorola Solutions Mobile VPN Client with problems that can occur and the proposed solutions to them.

Table 25: Mobile VPN Client Device-level Issues

Problem	Solution
Mobile VPN Gateway connection issues.	See Mobile VPN Gateway Connection Issues on page 133.
Configuration Fail status appears in Motorola Solutions Mobile VPN client.	Complete the following to manually clear data for Motorola Solutions Mobile VPN client: **1** On your Android Device, go to **Settings** → **Applications**. **2** Scroll down and tap **Motorola Solutions Mobile VPN** client. **3** Tap **Clear Data**. **4** Restart your Android Device and reconfigure Motorola Solutions Mobile VPN client by performing Accessing and Configuring Motorola Solutions VPN on Non-Motorola Devices on page 180. **NOTICE:** If your Motorola Solutions Mobile VPN client was pre-loaded on your Android Device, then the **Clear Data** option is disabled.

This page intentionally left blank.

Appendix C

Licensing Administration

MVPN Gateway licensing administration is typically used to increase or decrease user capacity on the MVPN Gateway. It is important to use a license with a capacity that is sized to the number of users (clients) communicating during day-to-day and during peak capacity. This scenario is not a relationship to the maximum number of users. The maximum number supported on the MVPN is 1250 users (clients) per service group, with 5000 total users (clients) total in a system with 4 service groups. From an agency perspective, the maximum number supported is typically much higher than what is required for day-to-day operations and peak usage at the agency. The MVPN Gateway is sized for the agency, and may never need to use the maximum number of users.

NOTICE: Clients using Remote Access profile establish individual VPN tunnels, which counts as individual use of license permissions when connected. Multiple VPN clients using a single Site To Site Profile count as a single use of license permissions.

The MVPN Gateway allows a margin of 5% additional client sessions (IKE sessions) compared to the licenses installed. This margin is needed since the MVPN Gateway may have client sessions that are greater in number than the actual active clients, and for peak usage conditions.

Available client licenses are configured with and without MOBIKE enabled. The license types are:

- Basic License - VPN only, in increments of client capacity, without Mobility (MOBIKE with application steering) enabled.
- Advanced License - VPN, in increments of client capacity, with Mobility (MOBIKE with application steering) enabled.

NOTICE: With the Basic license installed, client connection attempts to use “mobility” are ignored, and any associated VPN connection is dropped.

The MVPN Gateway limits the IKE sessions based on the total number of client license capacities. For example, if there are 50 licenses installed on an MVPN Gateway instance, the MVPN Gateway limits the IKE sessions to 50 (53 with 5% extra margin) for the gateway.

Consult with your Motorola Solutions service representative for capacity sizing for your installation. The capacity sizing may include typical operation and future expansion. For future expansion, projections of client usage for both day-to-day operations and peak usage must be considered.

Obtaining a License

For instructions for obtaining a license, see Obtaining Mobile VPN Gateway UUID for Licensing on page 188 and Retrieving License File from Motorola Licensing Server on page 188.

If needed, contact your Motorola Solutions service representative to discuss the technical aspects of the solution and the required compatible license.

Required information for each client capacity license:

- MVPN UUID
- Client capacity.
- If MOBIKE is enabled or not.

CAUTION: Use care when ordering and installing a new client license file. New license files overwrite the existing license file on the MVPN. It is possible to overwrite a large capacity client license file with a new, smaller capacity file. This situation may not be desired.

C.1
Obtaining Mobile VPN Gateway UUID for Licensing

Prerequisites: Obtain a CD/DVD for transferring information associated with the MVPN Gateway license keys.

When and where to use: Apply a new or update an existing client license.

IMPORTANT: The MVPN communications services are restarted during this procedure. Any client connections are dropped.

Procedure:

1. Log in to the Mobile VPN Gateway.

   See Logging on to the Mobile VPN Gateway on page 111.
2. At the command prompt, enter: `admin_menu`
3. At the **Main Menu**, enter the number associated with **Application Administration**.
4. At the **Application Administration** menu, enter the number associated with **Licensing Administration**.
5. At the **Licensing Administration** menu, enter the number associated with **Display Host UUID**.

   The host UUID output is of the format: `564D08E1-0E59-2D51-8680-53DF766F7A22`.
6. Record the UUID and store the information in a secure location.

   NOTICE: One license applies to one service group and should be associated with, and installed for a host UUID for VPN Gateway that ends with an odd number (e.g. 1, 3, 5, 7).

C.2
Retrieving License File from Motorola Licensing Server

This process comprises procedures for obtaining a client user license, logging on to the Licensing Portal, adding an Entitlement, and downloading the license to local storage.

Process:

1. After determining the number of service groups, the desired client capacity, the UUID, and whether MOBIKE feature is enabled, contact your Motorola Solutions service representative to obtain a client user license.

   See Obtaining a License on page 71. The resulting client user license files are transferred on CD/DVD media.
2. Perform Logging On to the Licensing Portal on page 188.
3. Perform Adding a New Entitlement on page 189.
4. Perform Generating and Downloading a License on page 190.

C.2.1
Logging On to the Licensing Portal

Prerequisites: Purchase the device license and wait for the e-mail containing necessary information from Motorola Solutions before attempting to log on to the Licensing Portal.

When and where to use: Use these steps to access the Motorola Solutions Licensing Portal.

Procedure:

1. In an internet browser, log on at https://licensing.motorolasolutions.com.
2. If you do not have an account on the licensing portal.
   a. Select **New User**.
   b. Enter the appropriate information in the required fields on the Self-Service Registration page.
   c. Click **Complete**.

The **Operations Portal** window appears.

Postrequisites: You are ready to activate your license or download a license file.

C.2.2
Adding a New Entitlement

When and where to use: Use these steps to map a new entitlement to an existing account.

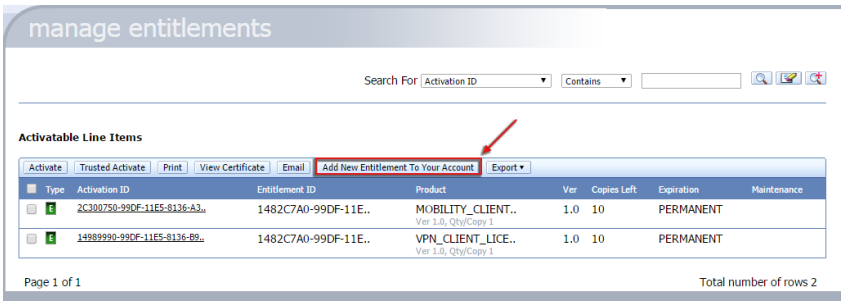
Process:

1. Log on to the licensing server and navigate to the **Operations Portal.**
2. In the Operations Portal, click **Manage Entitlements**.

   The **Manage Entitlements** window appears.

3. If you have a new Entitlement ID to map to your account, click **Add New Entitlement To Your Account**.

   Figure 23: Operations Portal — Manage Entitlements



   The **Add New Entitlement to Your Account** window appears.

4. Enter the new Entitlement ID in the ID field. Click **Map ID**.

   A message displays indicating that the Entitlement ID is successfully mapped.

5. Select **Manage Entitlements**.

   The **Manage Entitlements** window appears.

C.2.3
Generating and Downloading a License

NOTICE: The terms *client*, *device*, and *LTE device* apply to an instance of the MVPN Gateway virtual host.

When and where to use: Use these steps to generate and download the license file to local storage.

Process:

1 Log on to the Motorola Solutions Licensing Portal and navigate to the **Operations Portal**.

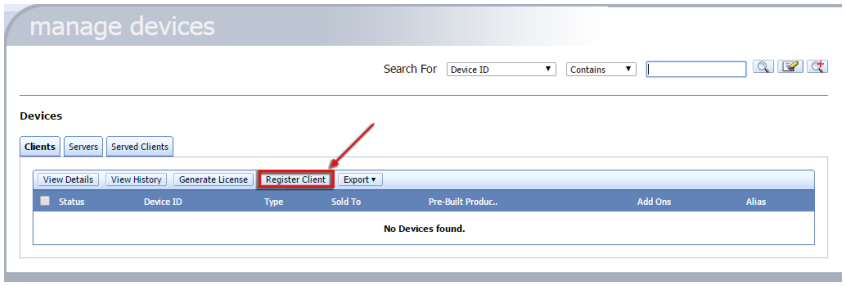
2 In the **Operations Portal**, click **Manage Devices**.

The **Manage Devices** window appears. If you have previously registered your device, it appears in the list.

3 If your device is new, register it.

a Click **Register Client**.

Figure 24: Manage Devices Tab — Register Client



The **Register Device** window appears.

b In the **Device ID** field, enter the VM UUID of the device.

The VM UUID is a 15-digit number which can be found on the sticker affixed to your LTE device. It may also be included in the properties list in the user interface for a device.

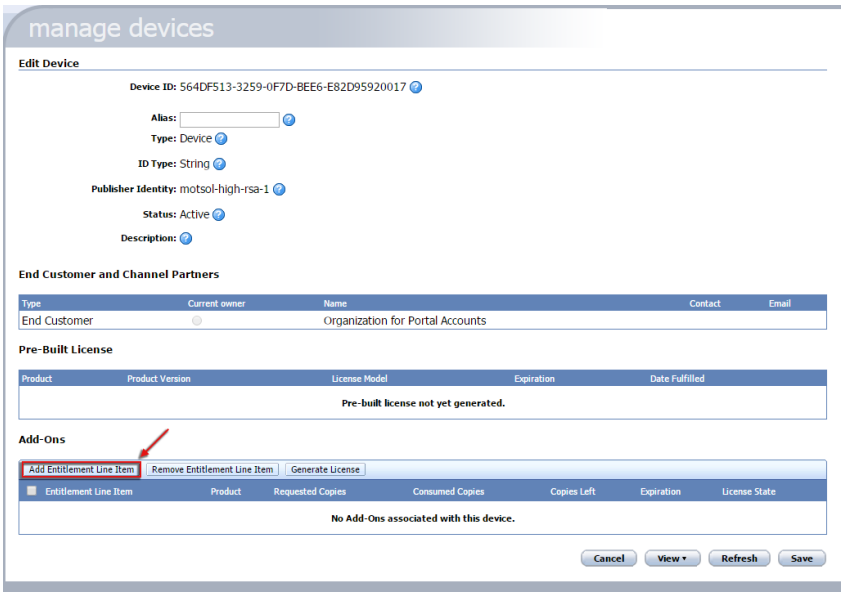
CAUTION: If you type the VM UUID incorrectly and click Submit, you cannot change it without contacting Motorola Solutions Support for assistance.

c From the **Host Type** list, select **Device**. Click **Submit**

The device is now created and the **Manage Devices** window appears.

4 Click **Add Entitlement Line Item**.

Figure 25: Manage Devices Tab — Add Entitlement Line Item



The **Select Line Item** window appears.

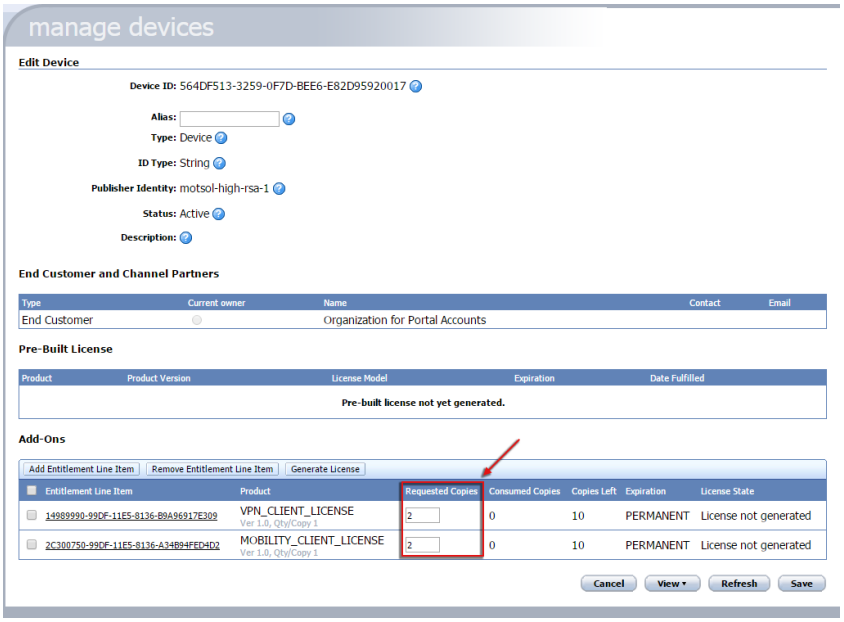
5 Select the check box for each Entitlement from the Entitlements you previously mapped to your account. Click **Save**.

You are returned to the **Manage Devices** window.

6 At the bottom of the **Manage Devices** window, enter the number of licenses to apply for each Entitlement Line Item.

NOTICE: If the Mobility option has been purchased, in the text field of the **Requested Copies** column, enter the same number for VPN_CLIENT_LICENSE and MOBILITY_CLIENT_LICENSE entitlement items.

Figure 26: Manage Devices Tab — Number of Requested Copies



7 Click **Generate License**.

You are asked whether you have a Request file.

8 Select **No**. Click **Generate**.

The **View Device Details** window appears with the details of your file.

9 Click **Download**.

You are prompted for a location to save the file. The file is saved with the .bin extension.

IMPORTANT: It is highly recommended that you rename the license file to reflect the VM UUID of the device.

10 Browse to the desired file location and click **Save**.

The file is saved with the .bin extension.

You are now ready to upload the license file to the device. See the device configuration guide.

C.3

Applying a License to a Virtual Machine

Prerequisites:

- Obtain a Mobile VPN Gateway UUID that is necessary for obtaining a license file. See Obtaining Mobile VPN Gateway UUID for Licensing on page 188
- Obtain a license file from the Motorola Solutions licensing portal. See Retrieving License File from Motorola Licensing Server on page 188.
- Create a CD/DVD for transferring information associated with the MVPN Gateway license keys.

When and where to use: Apply a new or update an existing client license.

IMPORTANT: The MVPN communications services are restarted during this procedure. Any client connections are dropped.

Procedure:

1 Log in to the Mobile VPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `admin_menu`

3 At the **Main Menu**, enter the number associated with **Application Administration**.

4 At the **Application Administration** menu, enter the number associated with **Licensing Administration**.

5 Insert a CD/DVD containing the MVPN Gateway license into the optical drive of the Windows-based local machine.

6 Mount the drive.

See Mounting a Drive in vSphere Client on page 112.

7 At the **Licensing Administration** menu, enter the number associated with **Install License Keys from CD/DVD**.

The system responds with a list of available licenses on the CD / DVD.

IMPORTANT: The new license file overwrites the previous license file. Ensure that the new license is of the desired capacity and license type. See Licensing Administration on page 70.

8 Select a license from the displayed list by entering the number shown with the license.

See step 9 for an example script output.

NOTICE: Several license numbers may be displayed. Record which license is used and store the information in a secure location. For redundant configurations, the main MVPN server communicates the licensing information to the back-up (redundant) server.

9 The server runs with an interactive script. Answer the prompts as displayed.

IMPORTANT: The MVPN communications services are restarted during this procedure. Any client connections are dropped.

Step example: IP addresses and license key numbers in the script output below are examples only.

```
Available License Files:

  1. /tmp/
xxxxx_Lic_564D08E1-0E59-2D51-8680-53DF766F7A22_20140807113432.bin

*Client Capacity - 400 users
*Mobility - Enabled
  q. Quit
Select license to apply (1-1,q): 1

WARNING
Loading a new license file will cause temporary service outage. Are
you sure you want to continue? (y/n) : y
Apply settings from /tmp/
xxxxx_Lic_564D08E1-0E59-2D51-8680-53DF766F7A22_20140807113432.bin
Stopping strongswan: Stopping strongSwan IPsec...
Starting strongswan: Starting strongSwan x.x.x IPsec [starter]...
                                                          [  OK  ]
License successfully added
License successfully added on secondary server
```

The server responds with the above success message and returns the user to the previous position in the admin menu.

10 Unmount the drive.

See Unmounting a Drive in vSphere Client on page 113.

11 To verify that the license was installed, perform Displaying the Virtual Machine License on page 193.

C.4 Displaying the Virtual Machine License

Perform this procedure to help determine any updates for the license capacity by displaying the current client license on the virtual machine.

Procedure:

1 Log in to the Mobile VPN Gateway.

See Logging on to the Mobile VPN Gateway on page 111.

2 At the command prompt, enter: `admin_menu`

3 At the **Main Menu**, enter the number associated with **Application Administration**.

4 At the **Application Administration** menu, enter the number associated with **Licensing Administration**.

5 At the **Licensing Administration** menu, enter the number associated with **Display License**.

The current license is displayed.

Step example:

```
License currently loaded:
*Client Capacity - 400 users
*Mobility - Enabled
```

Appendix D

Setting up the Active Directory Server for VPN Authentication

This chapter details configuration procedures relating to Windows Server and not relevant to core MPVN configuration.

D.1 Configuration Procedure Overview

Prerequisites:
Windows Server 2008 R2 is installed, with Active Directory Domain Services, ISS and DNS server configured.

Process:

1. Perform the Adding Network Policy Server Roles on page 195 procedure.
2. Perform the Generating the Network Policy Server CSR on page 196 procedure.
3. Transfer the Network Policy Server CSR to the PKI solution. The PKI solution returns the Network Policy Server certificate signed by the PKI solution TA.
4. Perform the Importing the Network Policy Server Certificate to the Active Directory Server on page 199 procedure.
5. Perform the Adding vpnusers for VPN Authentication to Active Directory Users and Groups on page 201 procedure.
6. Perform the Creating the RADIUS Clients and Adding a VPN Gateway Network Policy on page 202 procedure.
7. Perform the Enabling the Network Access Protection Agent on page 209 procedure.

D.2 Adding Network Policy Server Roles

Perform this procedure to add the network policy and access services.

Prerequisites:
Windows Server 2008 R2 is installed, with Active Directory Domain Services, ISS and DNS server configured.

Procedure:

1. Login to the Active Directory server with administrative privileges.
2. At the **Start** menu, type `server manager` in the search box.
3. Select the **Server Manager** application from the results.
4. Click **Server Manager**.
5. Click **Add Roles**.

   The **Add Roles Wizard** displays.
6. Select **Server Roles**.

7 Select **Network Policy and Access Services**.

8 Select **Network Policy Server**.

9 For the remainder of the **Add Roles Wizard**, click through the default values.

D.3
Generating the Network Policy Server CSR

Prerequisites: Perform the Adding Network Policy Server Roles on page 195 procedure.

Procedure:

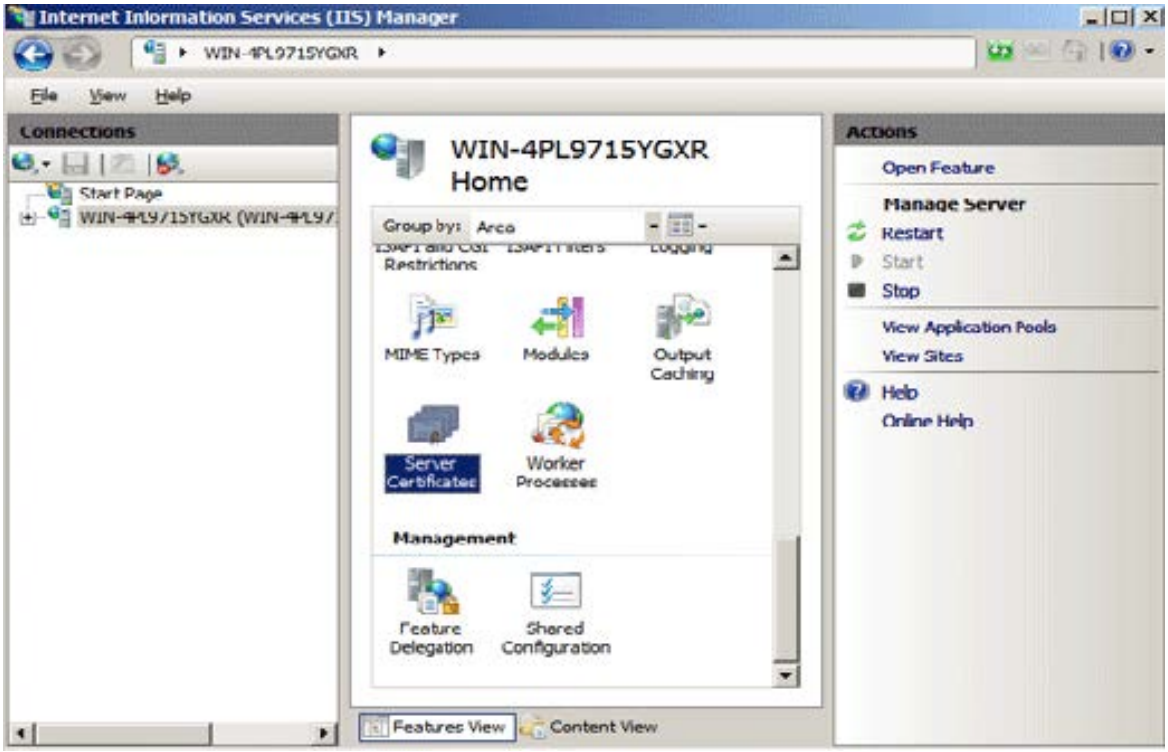
1 Login to the Active Directory server with administrative privileges.

2 Click **Start → Administrative Tools → Internet Information Services (IIS) Manager.**

3 Select the server name.

4 In the middle window, scroll down and double-click **Server Certificates** under the **Security** section.

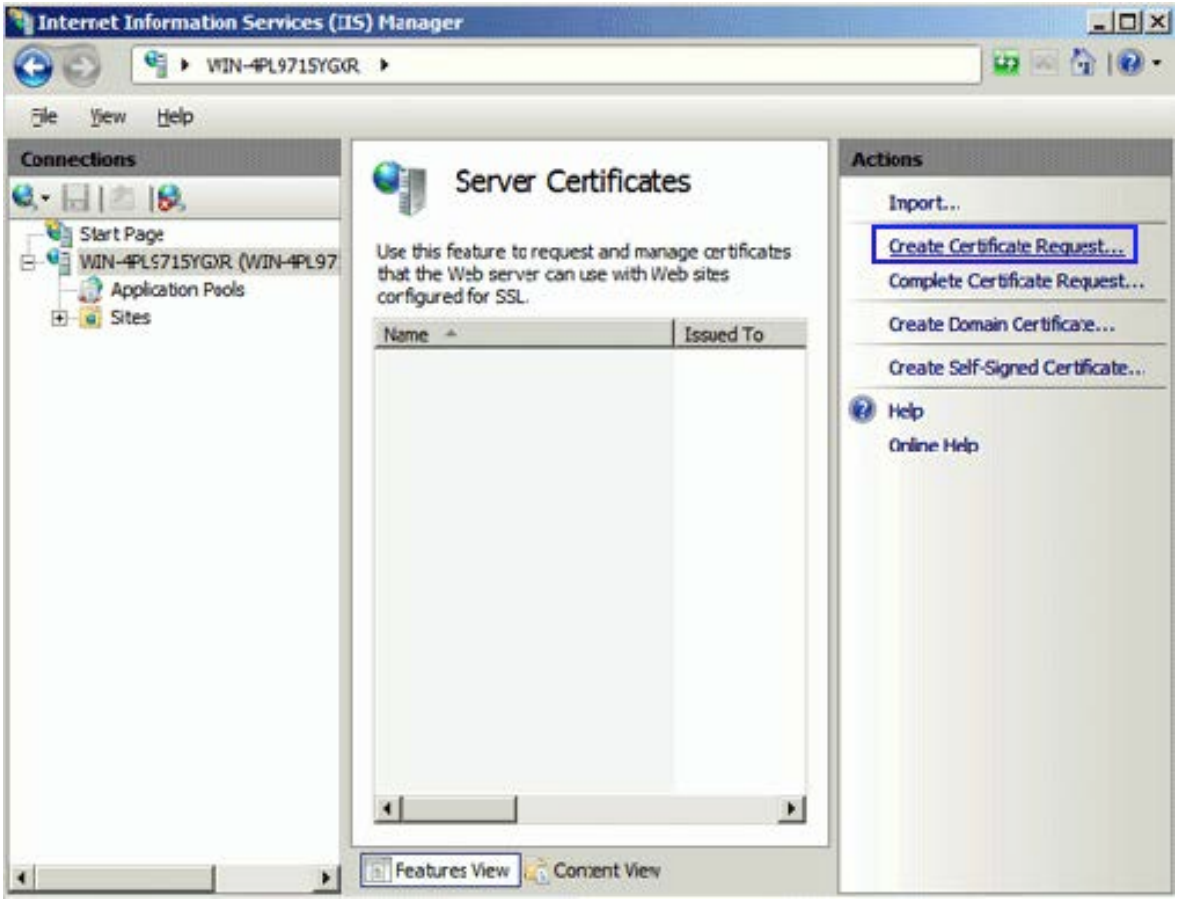
Figure 27: IIS Manager Server Window, Server Certificates Selection



5 Click **Create Certificate Request** in the **Actions** window of the right pane.

The **Request Certificate** wizard appears.

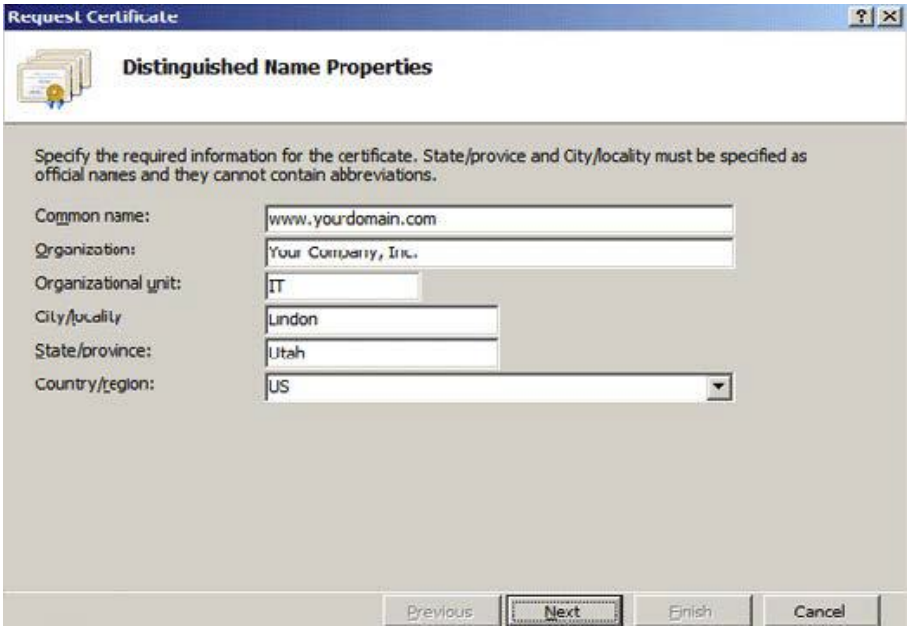
Figure 28: IIS Manager Create CSR Window



6 In the **Distinguished Name Properties** window, enter the following:

- Common Name - The name through which the certificate will be accessed. This is typically the fully qualified domain name, such as, `www.domain.com` or `mail.domain.com`.
- Organization - The legally registered name of your organization/company.
- Organizational unit - The name of your department within the organization (frequently this entry will be listed as "IT," "Web Security," or is simply left blank).
- City/locality - The city in which your organization/company is located.
- State/province - The state in which your organization/company is located.
- Country/region - Two-character country code.

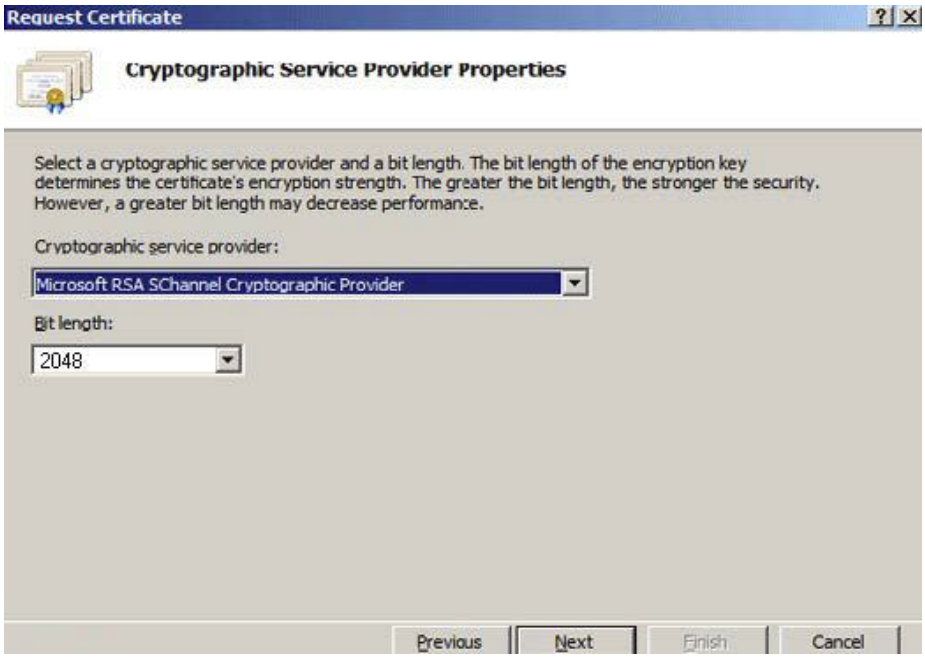
Figure 29: Distinguished Name Properties Window



7 Click **Next**.

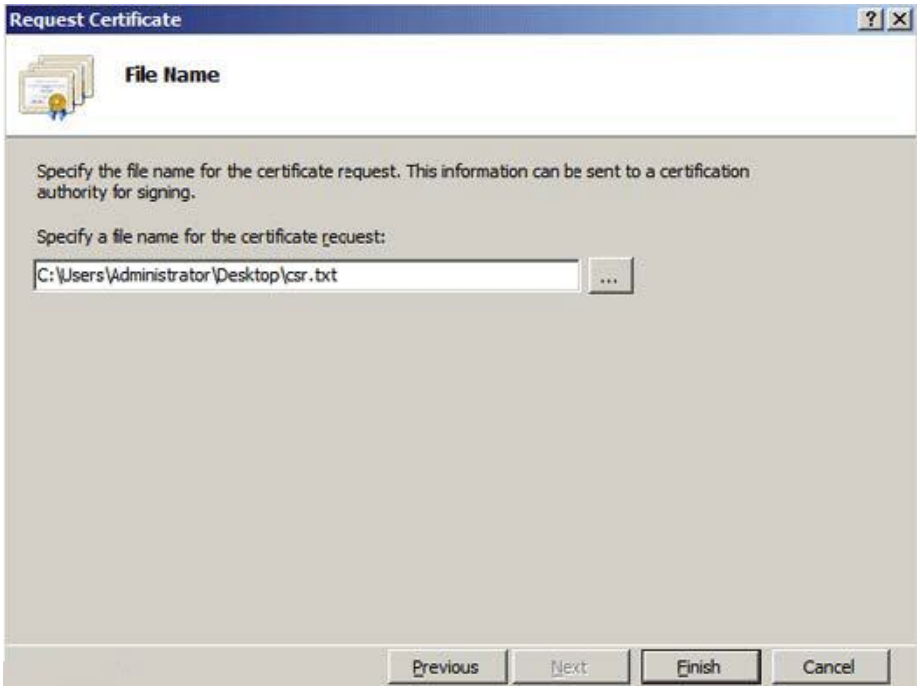
8 In the **Cryptographic Service Provider Properties** window, leave both settings at their defaults (Microsoft RSA SChannel and 2048) and click **Next**.

Figure 30: CSR Cryptographic Service Provider Properties Window



9 Enter a filename for the CSR.

Figure 31: CSR File Name Entry Window



10 Click **Finish**.

D.4

Importing the Network Policy Server Certificate to the Active Directory Server

Prerequisites:
Perform the Generating the Network Policy Server CSR on page 196 procedure.

The Network Policy Server CSR has been provided to a PKI solution which generated Network Policy Server certificates signed by a Trust Anchor.

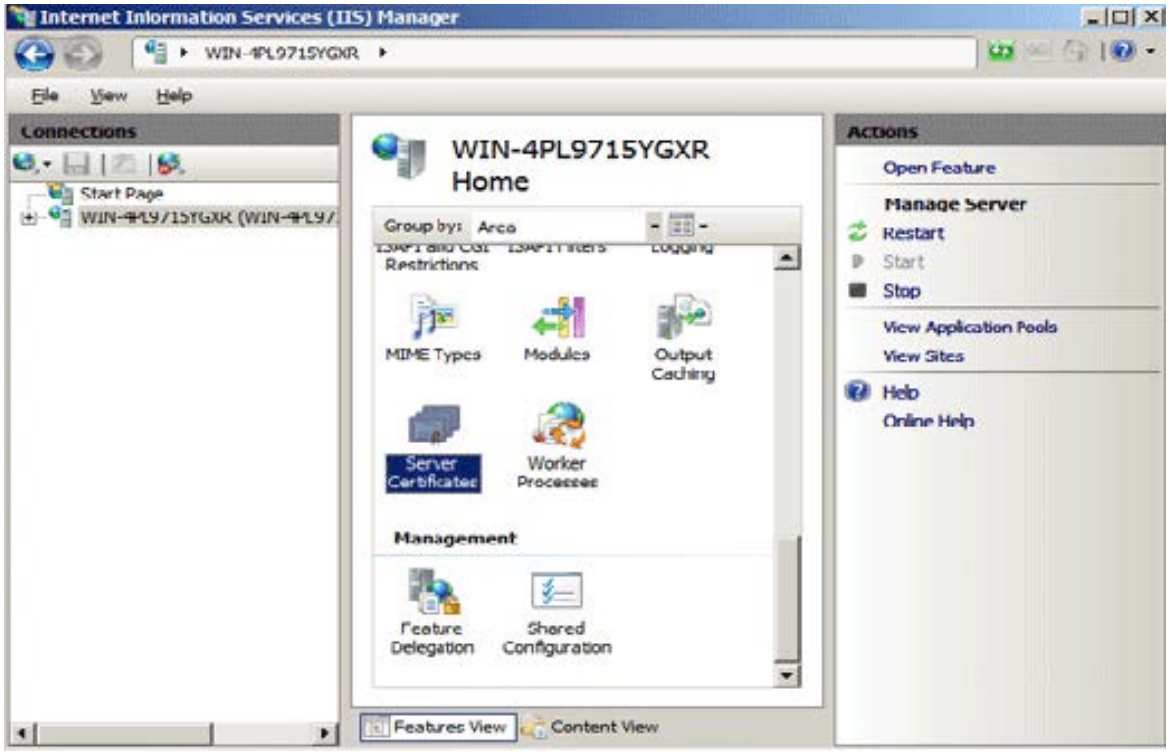
Procedure:

1. Login to the Active Directory server with administrative privileges. Transfer the signed Network Policy Server certificate to the server.

   Step example: `your_domain_name.cer`

2. Click **Start → Administrative Tools → Internet Information Services (IIS) Manager.**
3. Select the server name.
4. In the middle window, scroll down and double-click **Server Certificates** under the **Security** section.

Figure 32: IIS Manager Server Window, Server Certificates Selection



5 Click **Complete Certificate Request** in the **Actions** window of the right pane.

The **Complete Certificate Request** wizard appears.

Figure 33: IIS Manager Complete Certificate Request Window

6 Browse to the `your_domain_name.cer` file (from step 1) as provided from the PKI solution.

7 Enter a friendly name for the certificate.

The friendly name is not part of the certificate itself, but is used by the server administrator to easily distinguish the certificate.

Figure 34: Certificate Authority Response, Friendly Name Entry

8 Click **OK**.

The certificate is installed on the server.

NOTICE: There is a known issue in IIS 7 giving the following error: `Cannot find the certificate request associated with this certificate file. A certificate request must be completed on the computer where it was created`. Another message stating: `ASN1 bad tag value met` may also be displayed.. If this is the same server that you generated the CSR on then, in most cases, the certificate is actually installed. Cancel the dialog messages and press F5 to refresh the list of server certificates. If the new certificate is displayed in the list after the refresh, you can continue with the next step. If it is not in the list, you will need to re-issue the certificate using a new CSR.

D.5 Adding vpnusers for VPN Authentication to Active Directory Users and Groups

Prerequisites:

Perform Importing the Network Policy Server Certificate to the Active Directory Server on page 199.

See Configuration Procedure Overview on page 195.

When and where to use:

NOTICE: The user and group, **vpnuser1** and **vpnusers** are for example purposes only.

Procedure:

1 Login to the Active Directory server with administrative privileges.

2 At the **Start** menu, type `server manager` in the search box.

3 Select the **Server Manager** application from the results.

4 Select **Users**.

5 In the right pane, select **More Actions** → **New** → **Group**

6 Create a group. Enter: `vpnusers`

Keep the default for `group scope`.

7 In the right pane, select **More Actions** → **New** → **User**

8 Create a user. Enter: `vpnuser1`

9 Enter the user password.

10 Select the `Password never expires` check box.

11 Add the `vpnusers` group to the list of groups.

D.6

Creating the RADIUS Clients and Adding a VPN Gateway Network Policy

Prerequisites:

Perform Adding vpnusers for VPN Authentication to Active Directory Users and Groups on page 201.

See Setting Up MVPN Server to Client Authentication Including Active Directory on page 96.

Obtain the IP address for the RADIUS server (VPN Gateway Access Server) for the MVPN gateway.

Procedure:

1 Login to the Active Directory server with administrative privileges.

2 At the **Start** menu, type `server manager` in the search box.

3 Select the **Server Manager** application from the results.

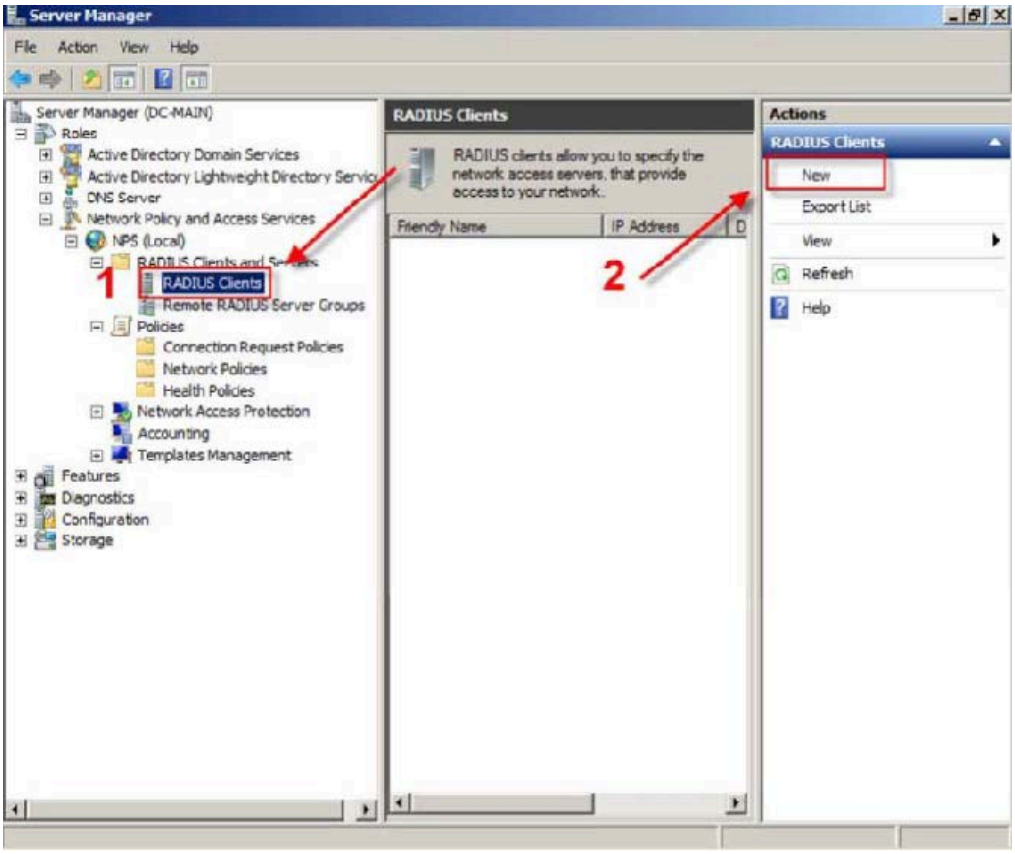
Adding MVPN RADIUS Clients

4 Obtain vpnint network IP of the MVPN gateway.

   a Select **Network Policy and Access Services** → **NPS (Local)** → **RADIUS Clients and Servers** → **RADIUS Clients** in the left pane.

   b In the right pane click **New** to add a new RADIUS client.

Figure 35: Server Manager Window



c In the **New RADIUS Client** dialog, enter a user friendly name (can be anything) for the new RADIUS client.

d Select the **Manual** check box.

NOTICE: The same shared secret must be used for MVPN Gateways from one Service Group.

e Enter a string, that is used as a “shared secret” password between the Active Directory server and MVPN Gateway.

The information is entered on the MVPN Gateway, as a “shared secret” during the Adding a RADIUS Server Configuration on page 98 procedure.

f Record the data used in this procedure and store the information in a secure location.

g Click **OK**.

h Repeat step 2 through step 4 g to add all the IP addresses of the remaining MVPN Gateway Servers.

Create the New Network Policy Wizard

5 In the **Server Manager** window, select **Network Polices** the left pane. Click **New** in the right pane.

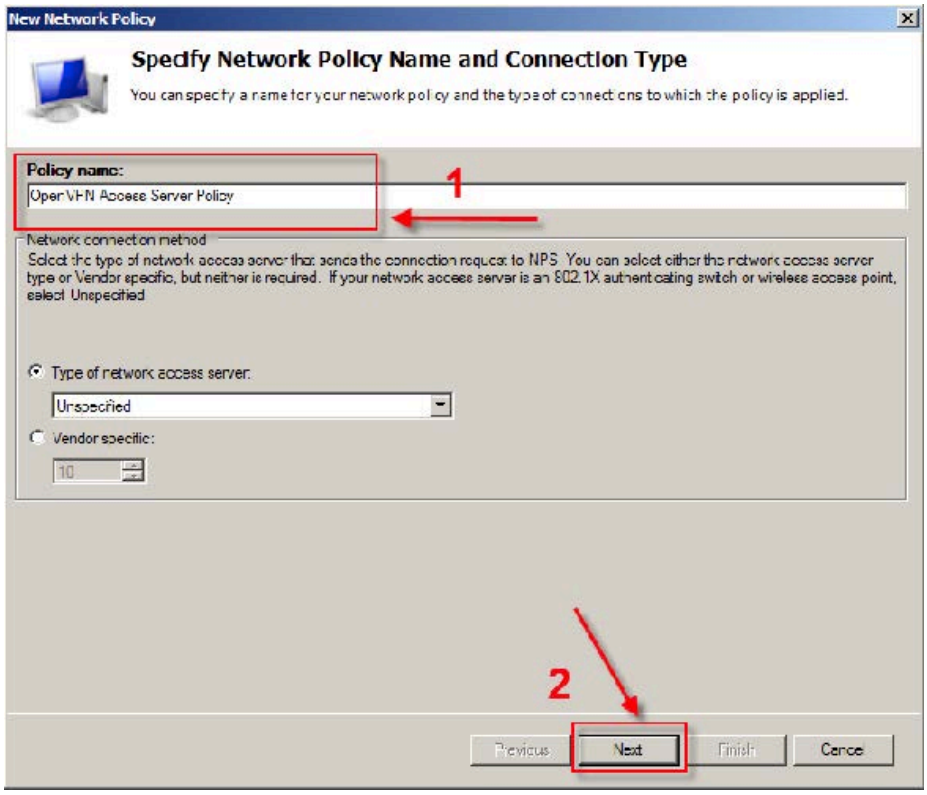
a Navigate to the Network Policies section underneath Policies. Click New on the right navigation pane.

b **Network Policy and Access Services → NPS (Local) → Policies → Network Policies**

c Click **New** in the right pane.

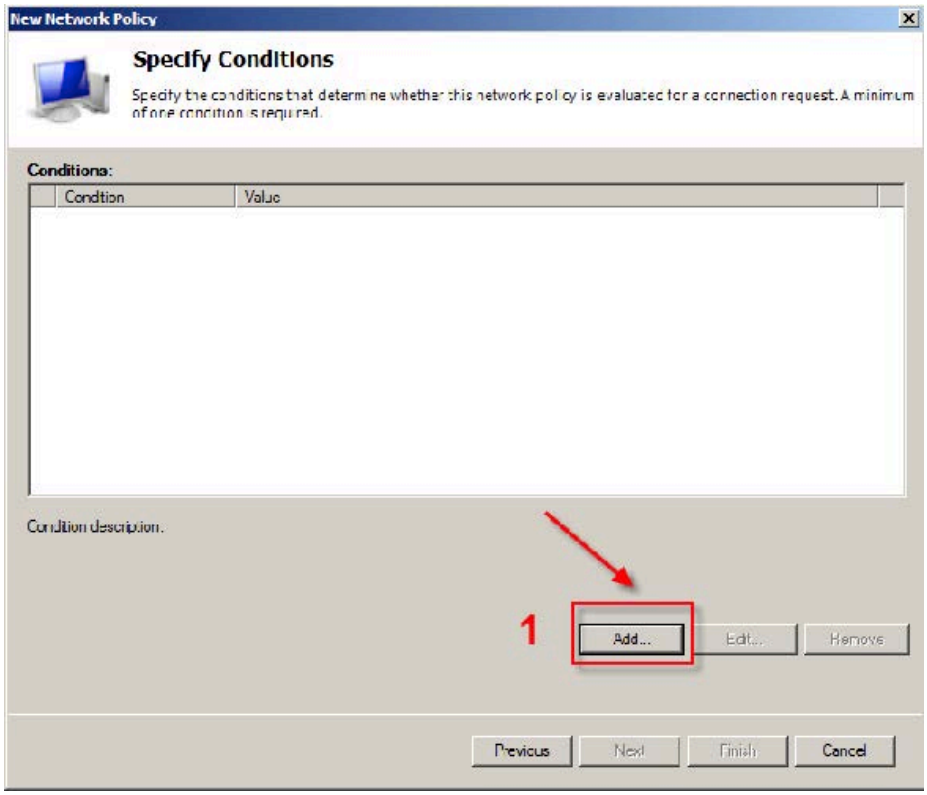
d In the **New Network Policy** dialog, enter a policy name for your new policy (this can be any name desired). Leave the server type as **Unspecified**. Click **Next**.

Figure 36: New Network Policy Window



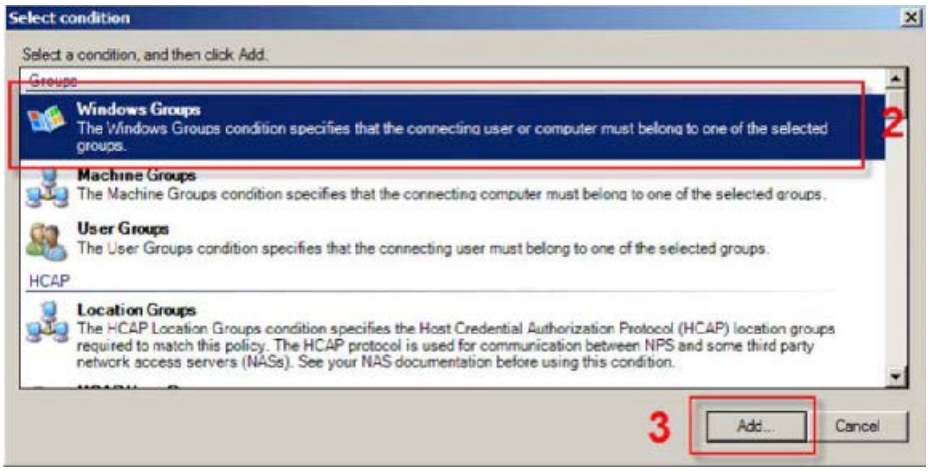
e In the **Specify Conditions** window, click **Add**.

Figure 37: New Network Policy – Specify Conditions Window



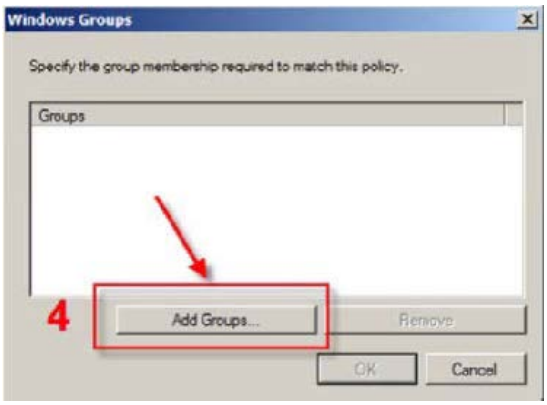
f In the **Select Condition** window, select **Windows Groups** and click **Add**.

Figure 38: Select Condition Window



g Click **Add Groups** to add new group memberships.

Figure 39: Windows Groups – Add Groups Window



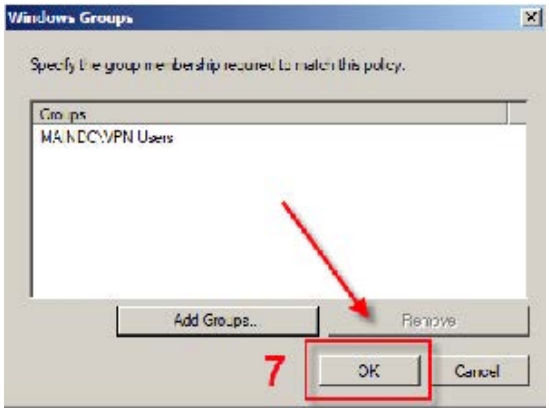
h Enter the group names you want to allow access to. Verify the entries. Click **OK**.

In this example, the group **vpnusers** are allowed access to the VPN.

Figure 40: Select Group Window

i In the **Windows Groups** window, click **OK**.

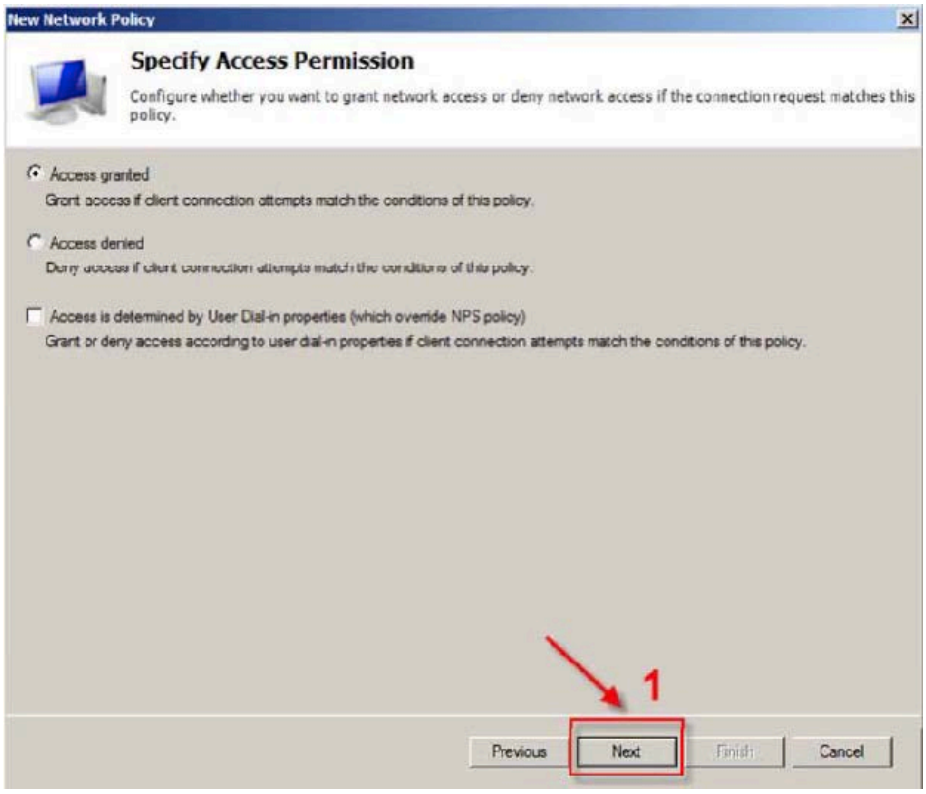
Figure 41: Windows Groups Window



j In the **New Network Policy** window, verify the entry in the **Specify Conditions** listing. Click **Next**.

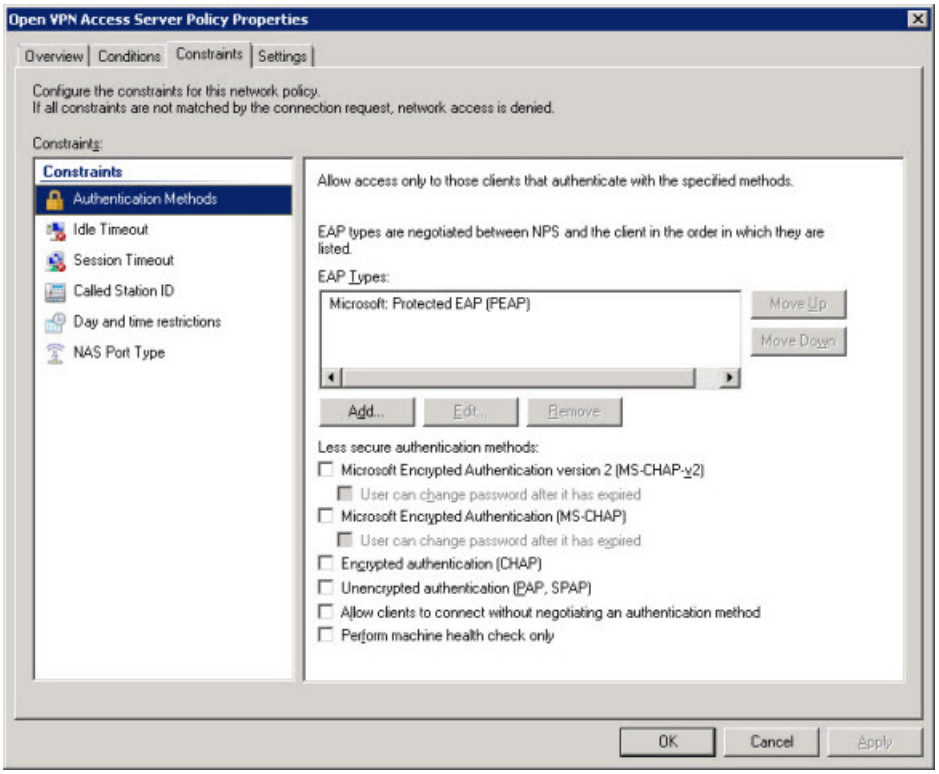
k In the **New Network Policy** window, accept the default `Access Permissions`. Click **Next**.

Figure 42: New Network Policy – Specify Access Permission Window



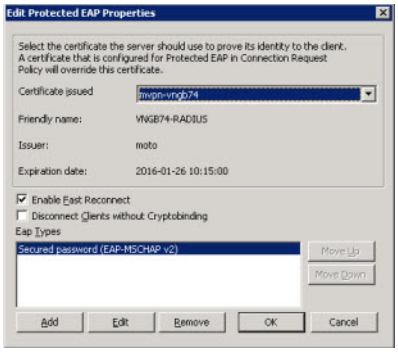
I In the **Open VPN Access Server Policy Properties** window, from the **Constraints** tab, select **Microsoft: Protected EAP (PEAP)** from the **EAP Types** window and click **OK**.

Figure 43: Add Network Policy 1



m In the **Edit Protected EAP Properties** window, in the **Certificate Issued** list, select the Certificate that was imported to Active Directory in Importing the Network Policy Server Certificate to the Active Directory Server on page 199.

Figure 44: Add Network Policy 2



n Confirm **Enable Fast Reconnect** checkbox is checked.

o Click **OK**.

p Click **Next**.

q Select to accept the default constraints.

r Click **Next**.

s Select to accept the default settings for the network policy.

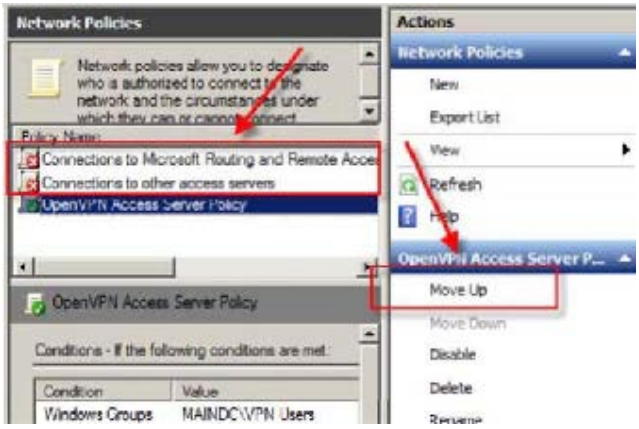
t Click **Next**.

u Click **Finish**.

The **New Network Policy** wizard closes.

6 In the **Server Manager**, look to see if the new network policy appears on the bottom of the **Network Polices** → **Policy Name** listing, this is a **Block** policy, denoted with a red “X”. Your clients cannot authenticate against the server. To fix this, select the newly created policy, and click the **Move Up** option on the right navigation pane, until your policy is above the default policies

Figure 45: Network Policies – Move Order of Network Policies Window



Register the Network Policy Server Using the NPS Console

7 Log on to the Network Policy Server (NPS) by using an account that has administrative credentials for the domain.

a Open the NPS console

b Right-click **NPS (Local)** → **Register server in Active Directory**

c The **Register Network Policy Server in Active Directory** dialog box displays.

d Click **OK**.

D.7
Enabling the Network Access Protection Agent

Prerequisites: Perform the Creating the RADIUS Clients and Adding a VPN Gateway Network Policy on page 202 procedure.

Procedure:

1. Login to the Active Directory server with administrative privileges.
2. Click **Start**, and enter `services.msc` in the search box.
3. In the **Services** window, double-click **Network Access Protection Agent**.
4. In the **Network Access Protection Agent** window, change the **Startup type** to **Automatic**, and click **Start**.
5. Click **OK**.

NOTICE: Wait for the **Network Access Protection Agent** service to start. This time is a few minutes between the completion of this procedure and the moment when the Active Directory server is ready to support authentication between the MVPN gateway and clients.

This page intentionally left blank.