



WatchGuard Mobile VPN License Server (MVLS)

Using an MVLS to manage WatchGuard Mobile VPN licenses

As of September 2019
WatchGuard Mobile VPN License Server: version 2.00

Using an MVLS to manage Mobile VPN Client licenses

About this Guide

This document is a guide to deploying a WatchGuard Mobile VPN License Server and using it to manage WatchGuard Mobile VPN licenses. For the most recent product documentation, see the WatchGuard web site at:

<http://www.watchguard.com/help/documentation/>.

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of

WatchGuard Technologies, Inc.
and NCP engineering GmbH.

About WatchGuard

WatchGuard offers affordable, all-in-one network and content security solutions that provide defense-in-depth and help meet regulatory compliance requirements. The WatchGuard Mobile VPN line enables secure IPsec VPN tunnels to be established to any Watchguard XTM network security appliance, and protects the associated personal computer with a firewall. WatchGuard extensible solutions scale to offer right-sized security ranging from small businesses to enterprises with 10,000+ employees. WatchGuard builds simple, reliable, and robust security appliances featuring fast implementation and comprehensive management and reporting tools. Enterprises throughout the world rely on WatchGuard signature red boxes to maximize security without sacrificing efficiency and productivity.

For more information, please call 206.613.6600 or visit www.watchguard.com.

Address

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

www.watchguard.com/support

U. S. and Canada:
+877.232.3531

All Other Countries:
+1.206.521.3575

Sales

U.S. and Canada:
+1.800.734.9905

All Other Countries:
+1.206.613.0895

Copyright, Trademark, and Patent Information

Copyright © 2019: NCP engineering GmbH. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

The WatchGuard Mobile VPN and the WatchGuard Mobile VPN License Server employ technology developed and owned by NCP and are sold under license by WatchGuard.

Contents

1. Introduction	5
2. Overview	5
2.1. WatchGuard Mobile VPN product licenses	5
2.2. Licensing WatchGuard Mobile VPN Clients using the MVLS	6
2.3. MVLS Operational Procedures	8
2.3.1. Recommended Backup and Restore Procedure.	8
3. Installing and Operating a WatchGuard Mobile VPN License Server	10
3.1. Installation Prerequisites	10
3.2. Installation	11
3.3. Operating the MVLS	13
3.3.1. Starting and Stopping the MVLS application/service	13
3.3.2. To login to the MVLS Administration Web Console.....	13
3.3.3. Overview of MVLS Administration Web Console Menu.....	14
4. Managing Licenses	15
4.1. Setting up the MVLS after Installation.....	15
4.2. Licensing a WatchGuard Mobile VPN Client.....	20
4.2.1. Licensing a WatchGuard Mobile VPN Client.	20
4.2.2. Licensing a WatchGuard Mobile VPN Client.	23
4.3. Transferring Licenses between Clients – License Bind and Unbind.....	25
4.4. Adding Additional License Bundles.....	26
4.5. Merging License Bundles for a specific product - Merge Bundles	28
4.6. License Activation when Updating to a Newer Version of WatchGuard Mobile VPN.....	30
4.7. Mobile VPN License Server Outages, and associated Client Recovery	31
4.8. Changing the MVLS Machine's IP Address - and Licensing Implications.....	32
4.8.1. Change the MVLS machine's IP address	32
4.8.2. Generate a new Initialization File.....	32
4.8.3. Relicense Affected Clients	33
5. Clients - Versions supported by this MVLS version	34
6. Document Revision Status	34

Using an MVLS to manage Mobile VPN Client licenses

1. Introduction

This manual describes:

- the management and distribution of licenses to large numbers of WatchGuard Mobile VPN (referred to in this document as Mobile VPN Client(s)):
WatchGuard Mobile VPN – Windows variant
WatchGuard Mobile VPN – Mac OS X variant
- the functionality provided by the WatchGuard Mobile VPN License Server (MVLS) in combination with those Mobile VPN Clients, and
- the procedures that must be undertaken by Virtual Private Network (VPN) administrators to manage the Mobile VPN Clients and their associated licenses.

2. Overview

The WatchGuard Mobile VPN License Server can be used to manage the distribution of licenses for the WatchGuard Mobile VPN Clients. Designed to simplify the management of software licenses for a large number of Mobile VPN Clients that make use of a VPN infrastructure, the MVLS maintains an inventory of licenses that have been purchased from WatchGuard, and manages the distribution of those licenses via the VPN to the respective Clients. By making use of an organization's VPN infrastructure, the licensing transactions between Client and MVLS are guaranteed to be secure against eavesdropping, tampering or theft.

2.1. WatchGuard Mobile VPN product licenses

Licenses to be managed via a Mobile VPN License Server are purchased from WatchGuard in bundles:

- A bundle is identified by a Bundle ID.
- A bundle contains a Bundle Key and a count of licenses represented by the bundle. The Bundle ID and Bundle Key are issued by WatchGuard in either paper or electronic form.
- All licenses represented by a bundle are associated with a specific WatchGuard Mobile VPN product: a specific WatchGuard Mobile VPN Client product and software version
or
a specific WatchGuard Mobile VPN Mac OS Client product and software version
- The information making up a bundle is downloaded from NCP's Activation Server in electronic form. During an initialization transaction between the Mobile VPN License Server and the NCP Activation Server, each license represented by the bundle is allocated a unique serial number.
- Each serial number can only bind the license for a specific product and software version of a Mobile VPN Client for an unspecified period of time.
- The serial number is bound to a specific Mobile VPN Client by running the Software Activation Wizard at a WatchGuard Mobile VPN Client machine (differences, in the software activation process, between Windows and Mac OS X variants is minimal),
- The serial number can be unbound from a specific machine, causing the associated license to be freed-up. That serial number may then be used to license that Client Product/Software Version on a different machine.
- Licenses, for the same product/software version set, purchased at different times can be merged together, thereby simplifying the management of an increasing number of Clients over time.

Using an MVLS to manage Mobile VPN Client licenses

2.2. Licensing WatchGuard Mobile VPN Clients using the MVLS

Licenses purchased for use with a Mobile VPN License Server are distributed to each WatchGuard Mobile VPN Client as follows:

- The licensing application – the Mobile VPN License Server - runs on a Microsoft Windows based server. At all times, the MVLS must be reachable from each Client via a VPN tunnel to the organization's VPN gateway.

NOTE: To ensure Clients can always communicate with it, the Mobile VPN License Server must be permanently connected to the organization's VPN infrastructure, i.e. it should be allocated an IP address reachable from the VPN infrastructure's IP subnet. Assignment can be either static at the server or dynamic via the organization's DNS service; if dynamic, the same DNS service MUST be accessible by all Client machines that are to be licensed via the MVLS.

NOTE: The Client builds an SSL (Secure Socket Layer) tunnel via the VPN tunnel to the Mobile VPN License Server. Firewalls and other security devices between the VPN gateway and the MVLS must be configured to allow traffic to reach port 12503 on the MVLS.

NOTE: As the Mobile VPN License Server must use the Internet to periodically communicate with NCP's Activation Server over HTTPS, a suitable route through corporate firewalls etc. to NCP's Activation Server (actsrv1.ncp.de) MUST always be available. Communication is via a Secure Socket Layer (SSL) VPN Tunnel to the NCP Activation Server, established by the MVLS; an HTTPS Proxy can be defined and used if necessary.

- The MVLS is administered via a secure web browser based administration interface – the Administration Web Console (web console). The connection between browser (see prerequisites) and web server (the MVLS) is secured via the Secure Socket Layer (SSL) protocol.

NOTE: By default, the MVLS web server uses port TCP/20132 for establishing this SSL link.

- The license bundle details provided by WatchGuard are entered into the MVLS database via the web console.
- After validating the bundle details with the NCP Activation Server and downloading the licenses from Activation Server to MVLS, an Initialization File is generated at the MVLS.

NOTE: Each Initialization File can only be used to license / activate the WatchGuard Mobile VPN Client product defined in the original bundle.

NOTE: The IP address (or fully qualified domain name if DNS is in use) of the MVLS is one of the items stored in this file. If, for any reason, the IP Address of the MVLS changes in the future, all Clients licensed via this MVLS (i.e. with the original IP Address) will no longer be able to communicate with the MVLS and will become un-licensed. Clients that become un-licensed (for whatever reason) CANNOT establish VPN connections. Thus if there is a chance that the MVLS IP Address is liable to change in the future, you are advised to allocate a Fully Qualified Domain Name to the MVLS and use DNS to distribute the IP address to Clients and VPN gateways.

See also

[Adding Additional License Bundles](#)

[Merging License Bundles for a specific product - Merge Bundles](#)

[MVLS Server Outages, Backups and Recovery](#)

and

[Changing the MVLS Machine's IP Address - and Licensing Implications](#)

Using an MVLS to manage Mobile VPN Client licenses

- The appropriate Initialization File must be downloaded to a portable media (CD/DVD, USB stick etc.) that can be transported to and used to activate any WatchGuard Mobile VPN Client that can connect to the organization's VPN gateway.
- At each Mobile VPN Client machine
 - the appropriate WatchGuard Mobile VPN Client software package must be installed, and
 - a Connection Profile which establishes a VPN tunnel to the VPN gateway must be tested and available,**before** starting to carry out the licensing process.
- Licensing of each Client using the MVLS should ideally be carried out during the standard 30 day evaluation period (which starts when the Client software is first installed). Activation can be performed later, but after expiry of the evaluation period a VPN tunnel can be established but only used for licensing / activation.
- The licensing process at the Mobile VPN Client uses information in the Initialization File, in combination with information from the MVLS, to bind a serial number to that Mobile VPN Client and license it. The actual Client licensing / activation is a two-step process:
 - i. A software activation routine imports the Initialization File from the Client device's file system into the Client software and the Client is marked as "Ready for Activation" - each Mobile VPN Client product incorporates a software activation feature, its exact operation is described in section 4.2 below.
 - ii. The next time the user establishes a tunnel to the VPN gateway, the Client detects the "Ready for Activation" status and exchanges licensing information with the Mobile VPN License Server. The Client is only fully licensed when this license details exchange process has been successfully completed.
- On licensing the Client, the MVLS database is updated with the following details:
 - WatchGuard Mobile VPN Client product and SW version number, and
 - Client IP address (and optionally its DNS name), and
 - serial number bound to that Client.
- The maximum number of Clients that can simultaneously each have a unique serial number bound to them is equal to the number of licenses purchased in the bundle plus any other bundles that have subsequently been merged with that bundle (see section [Merge Bundles](#)).
- Once the Client licensing process has successfully completed, that Client can establish and use a VPN tunnel to the organization's VPN gateway.
- A serial number may be unbound from a particular Client by using a web console command. The same Initialization File may then be used to bind that serial number to another Client by re-running the activation routine at that other Client.
- As the database of Client to serial number bindings is stored at the MVLS, each Client must periodically check its status at the MVLS, a check that is performed when the Client is connected to the VPN subnet.
- When a Client has been unbound from a serial number then use of the VPN tunnel by that Client is restricted to re-licensing the Client (by re-running the activation routine); no other VPN traffic is allowed.

Using an MVLS to manage Mobile VPN Client licenses

2.3. MVLS Operational Procedures

There are a number of individual activities that must be undertaken to ensure the trouble-free operation of the licensing service. These activities must be completely understood and corresponding procedures put in place before and during installation and commissioning of the MVLS.

2.3.1. Recommended Backup and Restore Procedure.

Details of serial number to Client address bindings are held online at the MVLS.

- If, for any reason, the MVLS fails (system failure causing the MVLS database to be lost), all Clients already bound to serial numbers will continue to be allowed access to the VPN gateway.
- However, all updates to the MVLS database will have been lost.

Due to this potential for loss of data it is recommended that a backup of the MVLS configuration folder (default location):

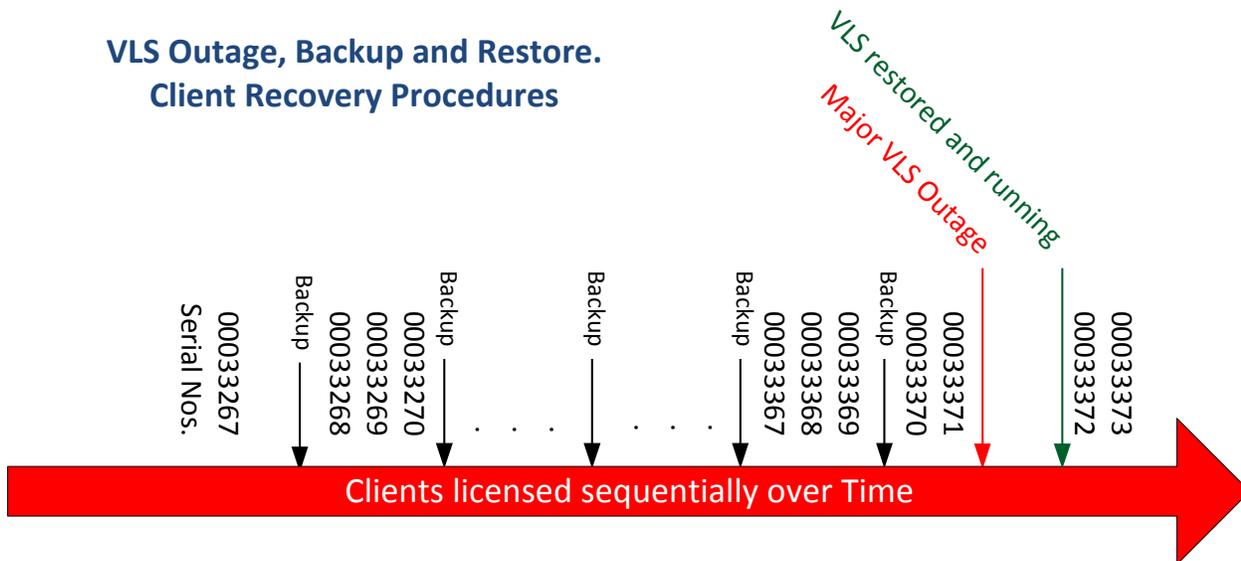
C:\Program Files\WatchGuard\Mobile VPN License Server\config

be performed on a regular basis.

If a MVLS outage occurs which requires a recovery:

- reinstall or recover the OS using standard procedures
- reinstall the Mobile VPN License Server software – see section 3
- copy the latest backup of the configuration MVLS folder to:
default location C:\Program Files\WatchGuard\Mobile VPN License Server\config
- The diagram on the next page illustrates details of any Client recovery procedures that might be necessary.

VLS Outage, Backup and Restore. Client Recovery Procedures



The diagram illustrates Mobile VPN Clients being licensed over time and an unexpected outage occurring on the MVLS. If backup and recovery procedures have been correctly followed, only those Clients licensed since the last backup will require re-licensing.

After the MVLS has been restored and is running again:

- Clients with serial numbers up to 00033369 will be able to continue using the VPN without interruption
- Clients with serial numbers 00033370 and 00033371 must be re-licensed:
 - immediately after the MVLS restore they will be able to continue establishing VPN connections successfully. However, some time later VPN connection establishment will fail as each Client's license will have been de-activated at that Client.
 - all subsequent attempts at such Clients to establish a VPN tunnel will fail with the "Client not licensed" message displayed, in red, in the Client Monitor, until the Client is re-licensed
 - until they are used to re-license Clients, serial numbers 00033370 and 00033371 will be marked as "available" in the MVLS web interface Licenses display
 - user support procedures should signal the MVLS Outage by issuing instructions to all users to re-license their Client if it was licensed since the time of the last backup (see recommendation in [MVLS Outage](#) section).
- the first two Clients to be licensed - or re-licensed as appropriate - would receive 00033370 and 00033371 respectively
- Clients that would receive serial numbers 00033372 and 00033373 will be licensed as normal.

Using an MVLS to manage Mobile VPN Client licenses

3. Installing and Operating a WatchGuard Mobile VPN License Server

3.1. Installation Prerequisites

<p>Mobile VPN License Server machine¹</p>	<p>Hardware: Any commercially available Intel X86 based machine. Backup Device: backup device with sufficient capacity to hold regular system backups – see section 2.</p> <p>Operating System: Microsoft Windows (32 or 64 bit) Server operating systems: MS Windows Server 2003 or later</p> <p>OS Services to be started or stopped: None specific to the MVLS service</p>
<p>Network Note: all IP routes must be available at all times</p>	<p>VPN Subnet: Each Mobile VPN Client must be able to access the MVLS via its VPN tunnel established to the VPN gateway.</p> <p>Client to MVLS IP access (Firewall port) - via VPN subnet: Port 12503/TCP on the MVLS machine must be accessible from each Client. This link is secured via an SSL tunnel between Client and MVLS.</p> <p>Internet: HTTPS connection to NCP Activation Server (actsrv1.ncp.de) An IP route between MVLS and NCP Activation Server MUST be available to allow the MVLS to periodically build an SSL VPN connection to the NCP Activation Server. An HTTPS proxy IP address can be configured at the MVLS to enable this connection if necessary.</p>
<p>Administration Web Console</p>	<p>Web Browser: Web browser host machine with Windows Internet Explorer V 8, or later Mozilla Firefox V 7 or later The web browser can optionally be hosted on the MVLS server machine if this has the necessary graphics support.</p> <p>Browser to Server Authentication Certificates: During MVLS installation, a self-signed browser–server certificate is automatically generated. This is used to authenticate the web console browser with the MVLS.</p> <p>Web Console to MVLS IP access (Firewall port): Port 20132/TCP on the MVLS machine must be accessible from the web console machine.</p>
<p>WatchGuard Mobile VPN Clients</p>	<p>The following Mobile VPN Clients can be licensed using a MVLS: WatchGuard Mobile VPN version 11.32 and later WatchGuard Mobile VPN Mac OS version 2.05 and later</p>

¹ WatchGuard strongly recommends AGAINST installing the MVLS and the VPN gateway software on the same physical machine - in such cases the MVLS service could potentially be visible to the Clients even when a VPN tunnel has not been established.

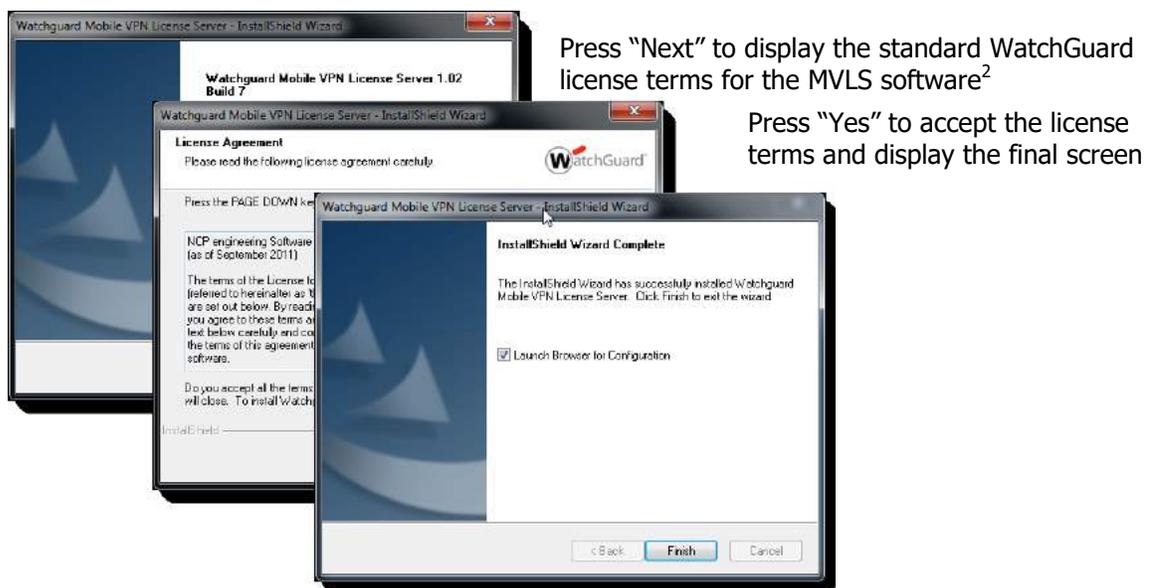
Using an MVLS to manage Mobile VPN Client licenses

3.2. Installation

Ensure that the MS Windows OS is completely installed on what will become the MVLS, that the network connections to Internet and VPN subnet are working and that the machine which will host the web console browser can access the MVLS. If the web console is to be run on the MVLS machine, the web browser to be used must be defined as the default browser.

(1) Install Mobile VPN License Server Software

- Download the MVLS installation package from the WatchGuard website as a compressed (zip) file
- Using Windows Explorer, browse to the download directory and unpack the downloaded file to a work directory.
- Browse to the work directory and execute the "WatchGuard_MVLS_Win3264_aaa_bbb.exe" file with administrator rights (RT mouse, run as administrator) to call the Installation Wizard.
(aaa = version number, bbb = build number)



- If the Administration Web Console browser is to be hosted on the MVLS server, ensure "Launch Browser for Configuration" is ticked and press "Finish". Continue at step c) below.
NOTE: this will launch the machine's default browser.
- If the web console browser is to be hosted on another machine, un-tick the "Launch Browser for Configuration", press "Finish" and continue with the next step.

² Note: not all diagrams in this document reflect the latest version of the MVLS software.

WatchGuard Mobile VPN License Server (MVLS)

Using an MVLS to manage Mobile VPN Client licenses

(2) Call the MVLS Administration Web Console

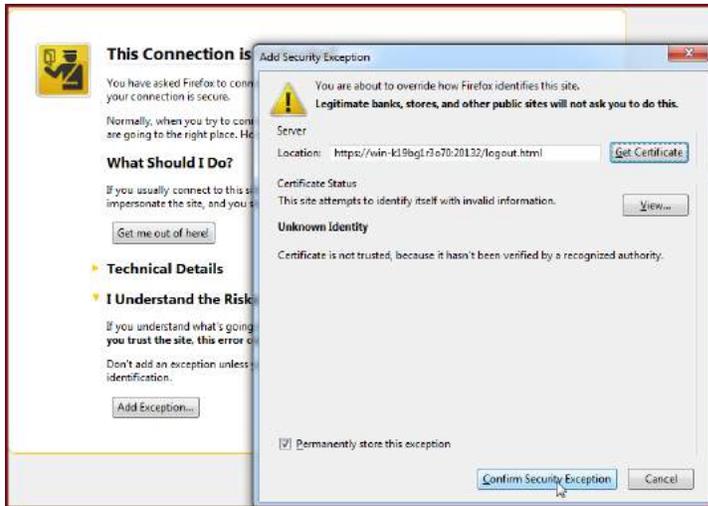
At the machine hosting the web console browser, start the browser and enter the following URL:

https://DNS_VLS:20132

where DNS_VLS is either the IP address or DNS name of the MVLS

(3) Web Browser <> Web Server Authentication

As an HTTPS URL has been entered, this invokes the HTTPS client <> server authentication process.



Accept the certificate exceptions at the browser and download the certificate to be used to mutually authenticate the browser and MVLS server.

(4) Define an MVLS administrator password

Enter the password to be used to authenticate logins to the MVLS:



Enter a suitable password and press "Set password"

This password will be requested in order to login to the MVLS in future.

The Mobile VPN License Server is now completely installed and ready for use.

Using an MVLS to manage Mobile VPN Client licenses

3.3. Operating the MVLS

All operational tasks associated with the MVLS must be carried out via the MVLS Administration Web Console. As this is web browser based it can be hosted either on the same physical machine as the MVLS or on a physically separate machine.

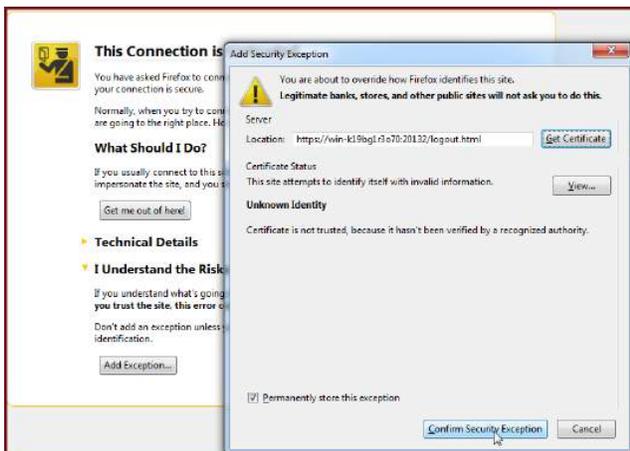
3.3.1. Starting and Stopping the MVLS application/service

The MVLS application/service is started and stopped automatically when the supporting machine/OS are booted and shutdown respectively. There are no special procedures for starting or stopping the MVLS application/service.

3.3.2. To login to the MVLS Administration Web Console

Enter the URL listed in b) above into the browser's address line.

If this is the first attempt to connect to the MVLS from this browser, the certificate download process must be carried out:



Get the certificate

and then

Confirm the security exceptions at the browser. (All subsequent connections between this the browser and MVLS will use the certificate to mutually authenticate each other.).

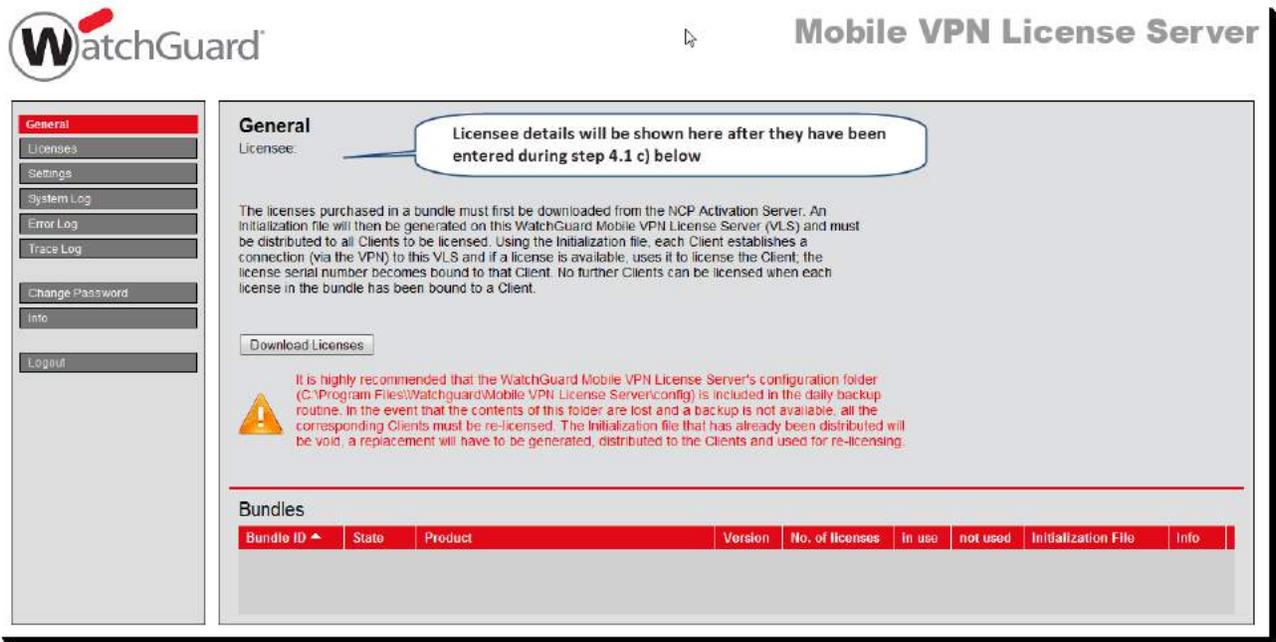
The Login screen is then automatically displayed.



WatchGuard Mobile VPN License Server (MVLS)

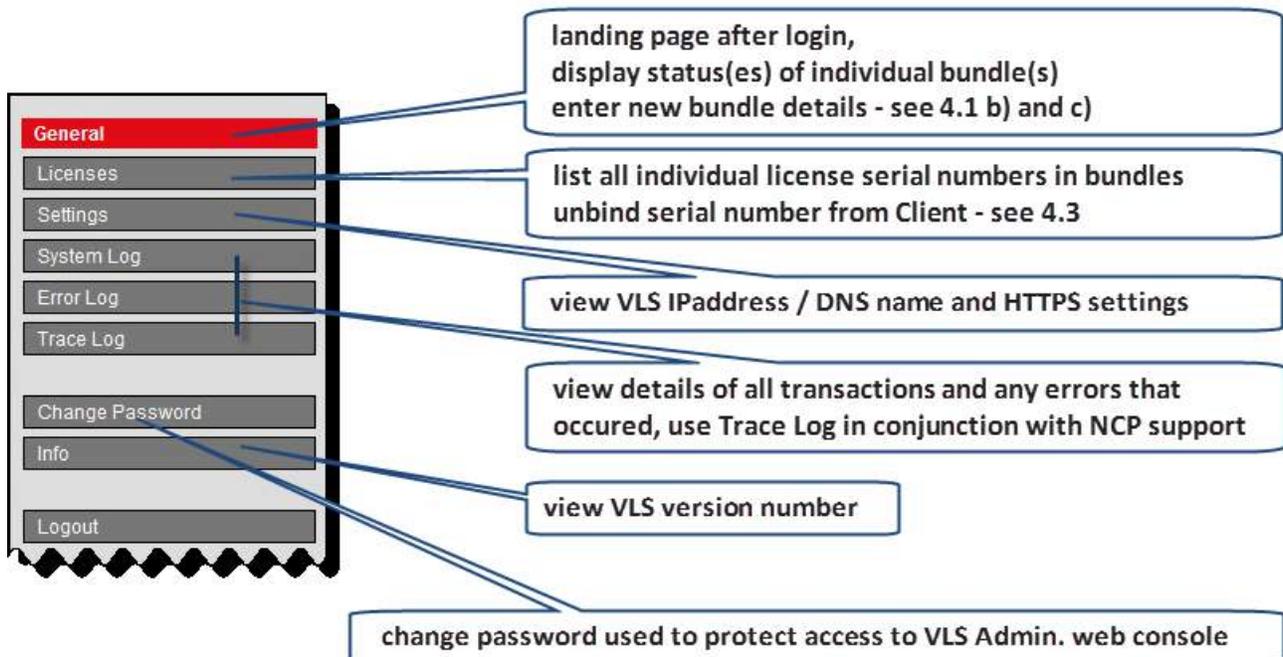
Using an MVLS to manage Mobile VPN Client licenses

The first screen displayed after login is the "General" screen.



3.3.3. Overview of MVLS Administration Web Console Menu

The MVLS is administered via the Administration Web Console menu. The functions of each menu item are:



4. Managing Licenses

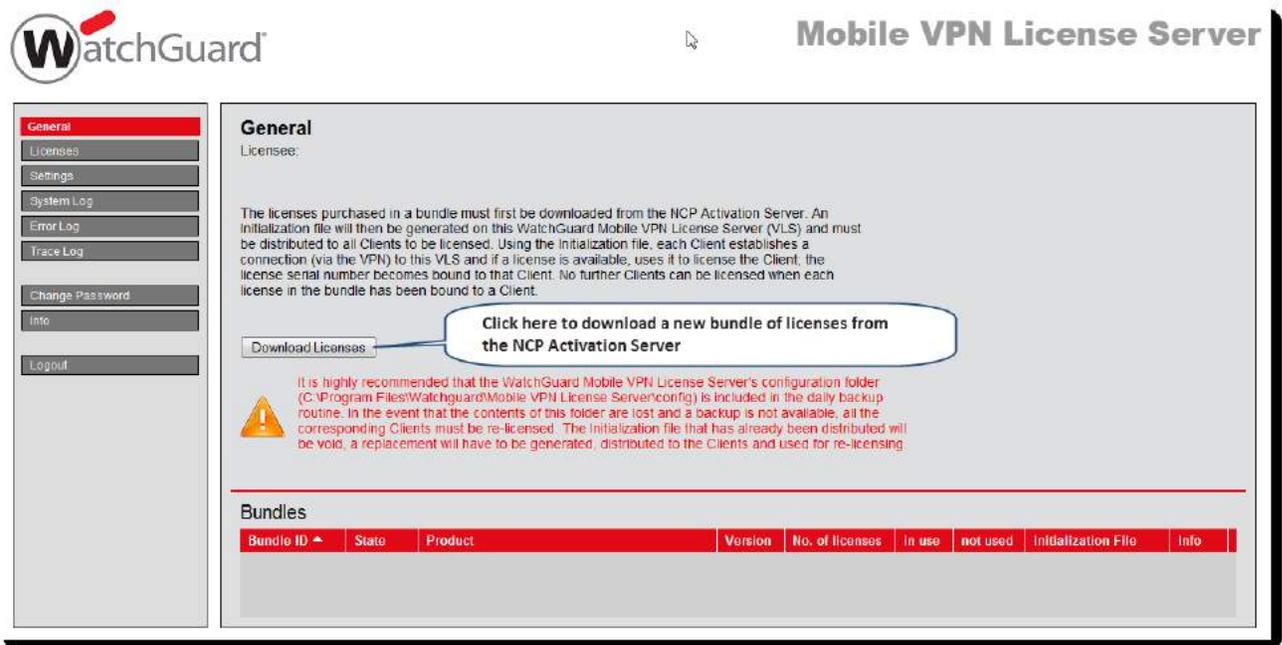
This section describes in detail how license bundles are downloaded to the Mobile VPN License Server and how Client licensing is performed

4.1. Setting up the MVLS after Installation

You will have received a document from WatchGuard giving the details of the License Bundle(s) you have purchased. Keep these at hand while you are carrying out the following steps

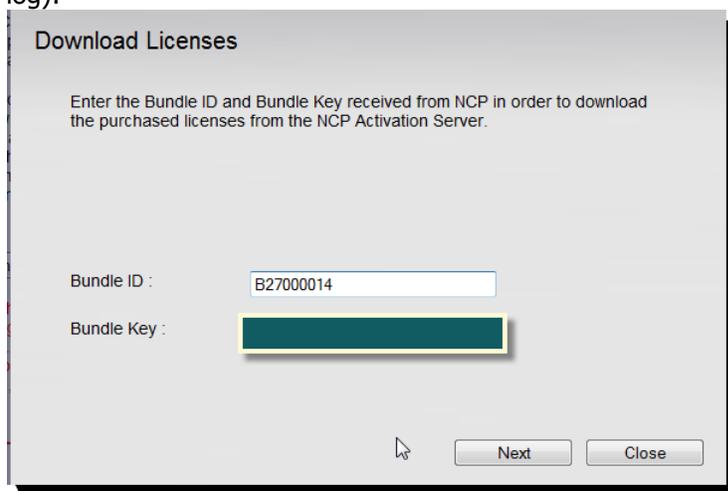
a) Login to the MVLS Web Console

Login to the MVLS web console using the browser, as described in section 3. The MVLS General screen is displayed but without any Licensee details (as this is the first time the MVLS has been accessed):



b) Enter Bundle Details

(If adding additional licenses, click General -> Download Licenses to display the "Download Licenses" dialog):



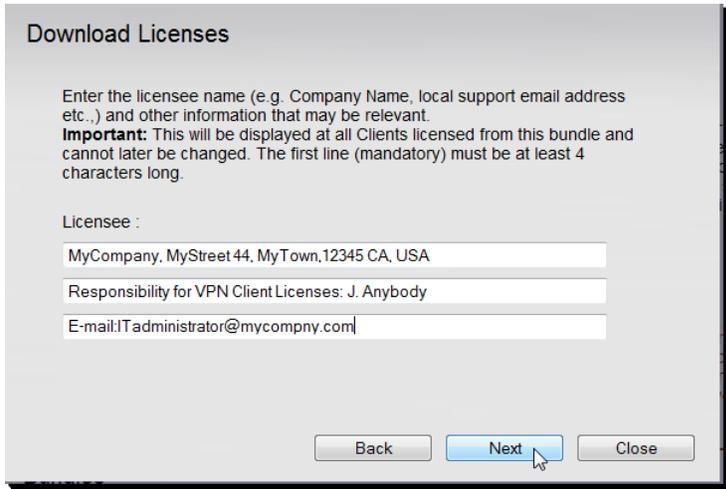
NOTE: Enter the details provided by WatchGuard in the respective fields

Press "Next" to continue. (If adding additional licenses, continue at [4.1 f](#))

Using an MVLS to manage Mobile VPN Client licenses

c) Enter Licensee Details (only if not yet entered)

As this is the first bundle being entered into the MVLS's database, you are now prompted to enter Licensee details. The 3 lines are free format and are displayed at each Client when it has been licensed.



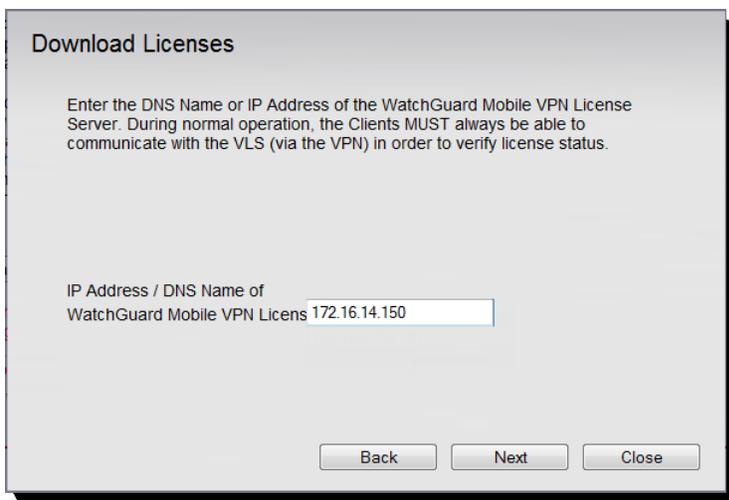
The screenshot shows a dialog box titled "Download Licenses". It contains the following text: "Enter the licensee name (e.g. Company Name, local support email address etc..) and other information that may be relevant. **Important:** This will be displayed at all Clients licensed from this bundle and cannot later be changed. The first line (mandatory) must be at least 4 characters long." Below this text are three input fields. The first field is labeled "Licensee :" and contains the text "MyCompany, MyStreet 44, MyTown,12345 CA, USA". The second field is labeled "Responsibility for VPN Client Licenses:" and contains "J. Anybody". The third field is labeled "E-mail:ITadministrator@mycompny.com". At the bottom of the dialog are three buttons: "Back", "Next", and "Close". A mouse cursor is pointing at the "Next" button.

NOTE: Once the information has been entered, it cannot be altered or deleted.

Check the details carefully before pressing the "Next" button.

d) Select or enter IP Address or enter DNS Name

Next select the IP Address by which all Clients will communicate with the MVLS. If a DNS Name is to be used for the server it must be entered here.



The screenshot shows a dialog box titled "Download Licenses". It contains the following text: "Enter the DNS Name or IP Address of the WatchGuard Mobile VPN License Server. During normal operation, the Clients MUST always be able to communicate with the VLS (via the VPN) in order to verify license status." Below this text is a single input field labeled "IP Address / DNS Name of WatchGuard Mobile VPN Licens" with the value "172.16.14.150" entered. At the bottom of the dialog are three buttons: "Back", "Next", and "Close".

Select an IP Address or enter the DNS Name and press "Next"

NOTE: Changing the IP Address of the MVLS machine at any time after it has been configured here will cause all currently licensed Clients to become unlicensed – those Clients would then be unable to undertake the regular validation of their licenses against the MVLS database. See section 4.5 for an overview of the actions involved in changing the IP address in this situation - however, you are advised to contact WatchGuard support if it becomes necessary to change the MVLS IP Address once Clients have been licensed.

WatchGuard Mobile VPN License Server (MVLS)

Using an MVLS to manage Mobile VPN Client licenses

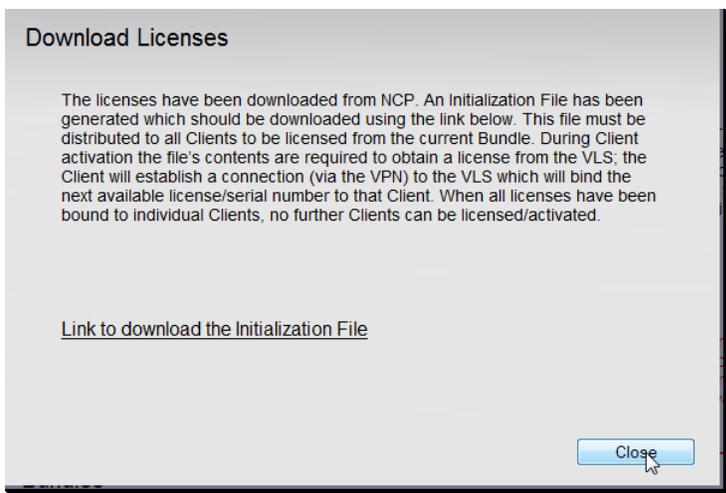
e) HTTPS Proxy to be used or not?

If an HTTPS proxy must be used to enable communications between the MVLS and the NCP Activation Server (see Overview Section 2.2), this must be enabled and the details entered here.



f) Download Licenses from NCP and generate Initialization File

At this point the MVLS establishes a connection to the NCP Activation Server and the license details associated with the bundle selected are downloaded to the MVLS. The Initialization File is then generated and can be downloaded to any media (USB stick etc.) accessible via the web console machine.



NOTE: If you wish to download the Initialization File immediately, click the link here and download the file (see details in Section 4.1 j) and press "Close",

otherwise just press "Close"

Using an MVLS to manage Mobile VPN Client licenses

g) License Details now stored in MVLS

The "General" screen is now re-displayed and now shows the Licensee details and an overview of the licenses associated with the bundle you purchase

General

Licensee: MyCompany, MyStreet 44, MyTown, 12345 CA, USA
 Responsibility for NCP Client Licenses: J.Anybody
 E-mail: ITadministrator@mycompany.com

The licenses purchased in a bundle must first be downloaded from the NCP Activation Server. An initialization file will then be generated on this WatchGuard Mobile VPN License Server (VLS) and must be distributed to all Clients to be licensed. Using the initialization file, each Client establishes a connection (via the VPN) to this VLS and if a license is available, uses it to license the Client, the license serial number becomes bound to that Client. No further Clients can be licensed when each license in the bundle has been bound to a Client.

[Download Licenses](#)

Warning: It is highly recommended that the WatchGuard Mobile VPN License Server's configuration folder (C:\Program Files\Watchguard\Mobile VPN License Server\config) is included in the daily backup routine. In the event that the contents of this folder are lost and a backup is not available, all the corresponding Clients must be re-licensed. The initialization file that has already been distributed will be void, a replacement will have to be generated, distributed to the Clients and used for re-licensing

Bundle ID	State	Product	Version	No. of licenses	In use	not used	Initialization File	Info
B27000014	valid	WatchGuard Mobile VPN (VL)	11.3	10	0	10	Download	Info

h) Displaying Bundle Details - Serial Numbers Used / Available etc.

To display all Serial Numbers that have been downloaded from the NCP Activation Server, press the "Licenses" menu tab. This displays all licenses for all bundles that have been registered with this MVLS.

Licenses

Serial Number: Hostname: [Search](#) [Unbind License](#)

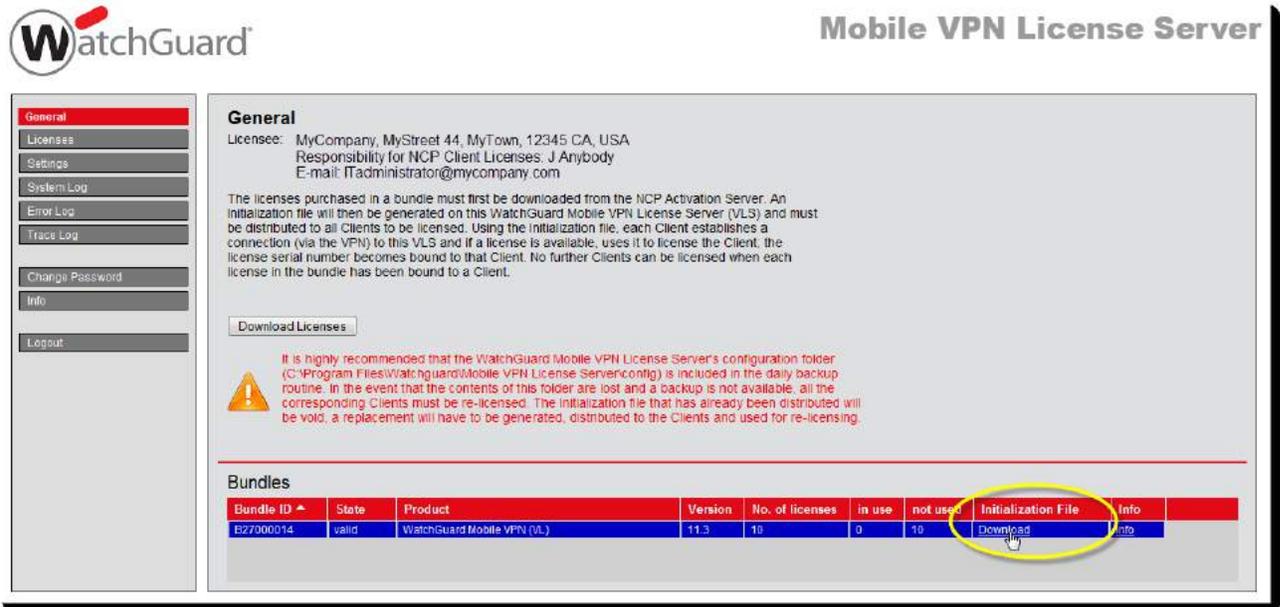
Items per page: 100 | 1

Serial Number	Bundle ID	Product	Version	State	Hostname	Last connect
27000015	B27000014	WatchGuard Mobile VPN (VL)	11.3	available		
27000016	B27000014	WatchGuard Mobile VPN (VL)	11.3	available		
27000017	B27000014	WatchGuard Mobile VPN (VL)	11.3	available		
27000018	B27000014	WatchGuard Mobile VPN (VL)	11.3	available		
27000019	B27000014	WatchGuard Mobile VPN (VL)	11.3	available		
27000020	B27000014	WatchGuard Mobile VPN (VL)	11.3	available		
27000021	B27000014	WatchGuard Mobile VPN (VL)	11.3	available		
27000022	B27000014	WatchGuard Mobile VPN (VL)	11.3	available		
27000023	B27000014	WatchGuard Mobile VPN (VL)	11.3	available		
27000024	B27000014	WatchGuard Mobile VPN (VL)	11.3	available		

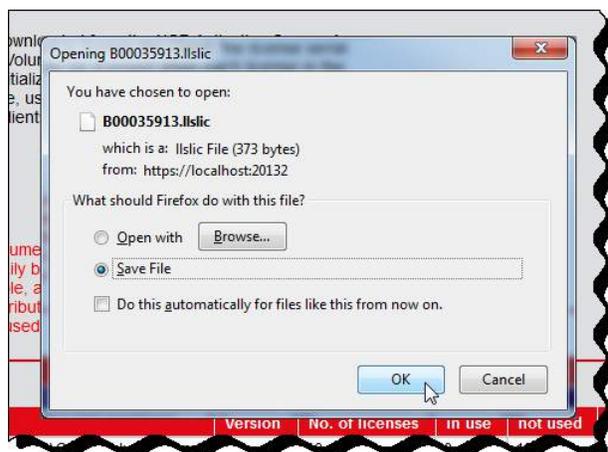
Using an MVLS to manage Mobile VPN Client licenses

i) Downloading the Client Initialization File

The Client Initialization File can be downloaded at any time. Call up the “General” screen and proceed as follows:



Select the “Download” link of the bundle Initialization File which you wish to create and press RT mouse.



In the browser’s download window select the “Save file” option and browse to the location where you wish to save the file. This is the file that will be used for [Licensing the Clients](#) – see Section 4.2

NOTE: This file can only be used to license Clients that correspond to the Product and Version Number defined in the original bundle.

Using an MVLS to manage Mobile VPN Client licenses

4.2. Licensing a WatchGuard Mobile VPN Client

The following items must be distributed to each Client to be licensed:

- Initialization File created in step [4.1 i](#))
- .wgx format Connection Profile file (also referred to as a User Profile file)
- a key/passphrase used to decrypt the Connection Profile file.

The exact distribution method is not described in this document as it is customer dependent.

The procedure to be followed is dependent on the type of Mobile VPN Client being licensed.

4.2.1. Licensing a WatchGuard Mobile VPN Client.

a) Check IP Connection to VPN gateway

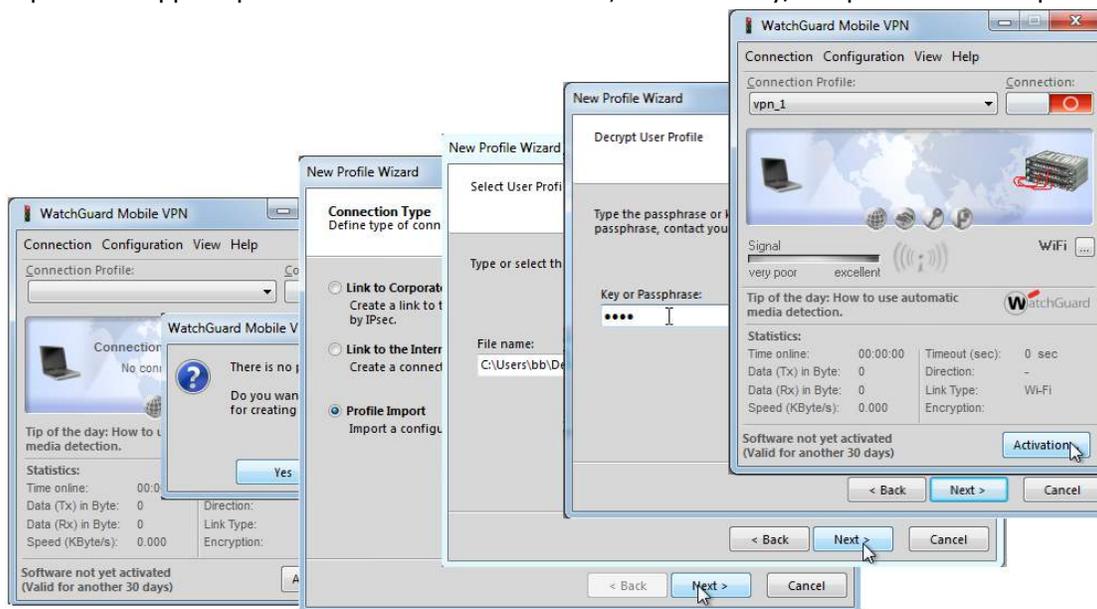
Once the OS on the Client machine has been installed, check that the connection to the IP communications network is working correctly.

b) Install WatchGuard Mobile VPN Client software

- Install the WatchGuard Mobile VPN Client software using standard WatchGuard installation procedures.
- When rebooted after the software installation, the Client software is automatically started and the monitor displayed - this makes use of the 30 day free-trial license delivered with the Client.

c) Import the Connection/User Profile (.wgx format file provided by System Administrator)

- Copy the supplied .wgx file to a convenient location (desktop in the illustration below).
- Whenever the software is started without a Connection Profile having first been created, the user is prompted to create one. Select "Yes", "Profile Import" and then use the Import Wizard's browser to import the supplied profile from the location chosen; enter the Key/Passphrase when requested.



- The Connection Profile imported will be used to establish a VPN connection via which the Client software will be licensed - described in step 4) below. Thus it is important that the Connection Profile parameters in the .wgx file are correct; errors could result in the Client being installed but not licensed.

Using an MVLS to manage Mobile VPN Client licenses

d) License the WatchGuard Mobile VPN Client Software

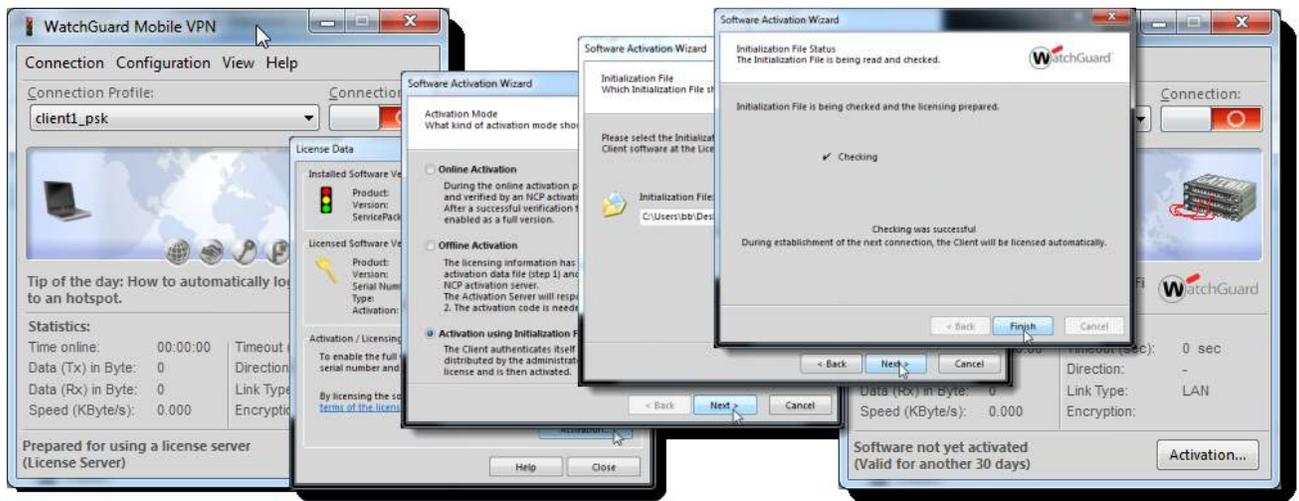
Licensing an individual WatchGuard Mobile VPN Client is a two-step process as follows:

(1) Import the Initialization File and run the software activation process

There are two methods for importing the Initialization File, either:

i. Use the Software Activation Wizard

- Copy the Initialization file to a convenient location



- Click the "Activation" button to call the Activation Wizard
- Select "Activation using Initialization File", follow the prompts to browse to the location of the Initialization File, and select that file.

or

ii. Restart the Client Monitor with the Initialization File stored in the Client's installation directory

- Stop the Client
- Copy the Initialization File to the Client's installation directory (default: C:\Program Files (x86)\WatchGuard\Mobile VPN)
- Re-start the Client.

Note: The copy of the Initialization File stored in the installation directory will be deleted after being read if this second method is used.

Regardless of which method is used:

- The contents of the Initialization File are checked and if valid, the "Check Successful – Licensing will be completed when the next VPN connection is established." message is displayed by the Wizard.
- The activation status is displayed in the lower frame of the Client Monitor:



Using an MVLS to manage Mobile VPN Client licenses

- (2) Complete the Client licensing by exchanging licensing details between Client and MVLS via the Corporate VPN

Establish a tunnel to the VPN gateway using the Connection/User Profile imported during step 3) above. During connection establishment the following takes place automatically:

- i. the Client establishes a connection to the VPN gateway - the yellow, "connection being established bar" is displayed
- ii. when the VPN tunnel is established, the Client Licensing software establishes a connection to the Mobile VPN License Server - the connection bar changes from yellow to orange.
- iii. The next available license (serial number) will be selected and licensing details transmitted to the Client – the connection bar changes from orange to green.



Licensing is now complete for this Client, indicated by the licenses status no longer being displayed in the lower frame.

From this point onwards the WatchGuard Mobile VPN Client is fully licensed and can establish VPN connections as required. No further activity is required in connection with licensing UNLESS there is an outage at the Mobile VPN License Server – see section 4.4.

NOTE: If an attempt is made to license a Client when all the licenses in a bundle have been used, then the message "Licensing operation failed" will be displayed and logged.

NOTE: In steps ii. & iii. above, if a VPN connection is established and the onwards connection to the MVLS is established immediately, the connection bar will only flash orange briefly before switching to green.

NOTE: In step ii. above, if a VPN connection is established but the onwards connection to the MVLS cannot be established, the connection bar will remain orange. Check that the MVLS is reachable from the VPN.

Using an MVLS to manage Mobile VPN Client licenses

4.2.2. Licensing a WatchGuard Mobile VPN Mac OS X Client.

a) Check IP Connection to VPN gateway

Once the OS on the Client machine has been installed, check that the connection to the IP communications network is working correctly.

b) Install WatchGuard Mobile VPN Client software

- Install the WatchGuard Mobile VPN Mac OS X Client software using standard WatchGuard installation procedures.
- When rebooted after the software installation, the Client software is automatically started and the monitor displayed - this makes use of the 30 day free-trial license delivered with the Client.

c) Import the Connection/User Profile (.wgx format file provided by System Administrator)

- Copy the supplied .wgx file to a convenient location such as the desktop
- Import the profile by dragging and dropping it onto the Client monitor; enter the .wgx passphrase when prompted.

Note: whenever the software is started without a Connection Profile having first been created, the user is prompted to create one. Select "Yes", "Profile Import" and then use the Import Wizard's browser to import the supplied profile from the location chosen; enter the Key/Passphrase when requested.

- The Connection Profile imported will be used to establish a VPN connection via which the Client software will be licensed - described in step 4) below. Thus it is important that the Connection Profile parameters in the .wgx file are correct; errors could result in the Client being installed but not licensed.

d) License the WatchGuard Mobile VPN Mac OS Client Software

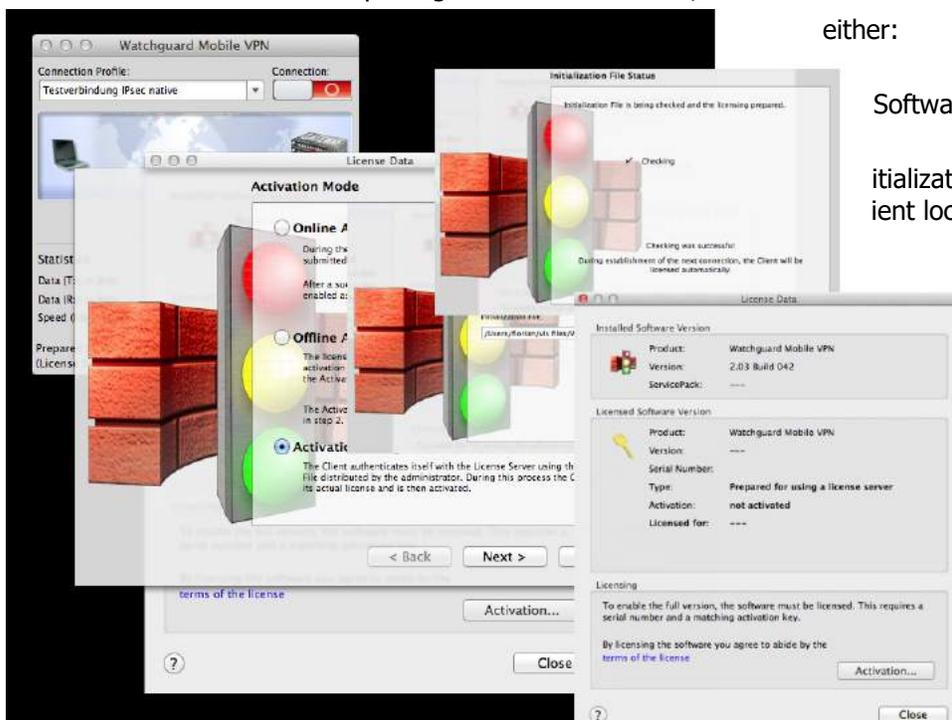
Licensing an individual WatchGuard Mobile VPN Mac OS Client is a two-step process as follows:

(3) Import the Initialization File and run the software activation process

There are two methods for importing the Initialization File,

either:

- i. Use the Software Activation Wizard
 - Copy the Initialization file to a convenient location



- Click the "Activation" button to call the Activation Wizard

WatchGuard Mobile VPN License Server (MVLS)

Using an MVLS to manage Mobile VPN Client licenses

- Select "Activation using Initialization File", follow the prompts to browse to the location of the Initialization File, and select that file.

or

- ii. "Drag and drop" the Initialization File from a directory to the Client monitor. This automatically initiates the Software Activation Wizard as in i. above.

Regardless of which method is used:

- The contents of the Initialization File are checked and if valid, the "Check Successful – Licensing will be completed when the next VPN connection is established." message is displayed by the Wizard.
- The activation status is displayed in the lower frame of the Client Monitor:



- (4) Complete the Client licensing by exchanging licensing details between Client and MVLS via the Corporate VPN

Establish a tunnel to the VPN gateway using the Connection/User Profile imported during step 3) above. During connection establishment the following takes place automatically:

- iv. the Client establishes a connection to the VPN gateway - the yellow, "connection being established bar" is displayed



- v. when the VPN tunnel is established, the Client Licensing software establishes a connection to the Mobile VPN License Server - the connection bar changes from yellow to orange.



- vi. The next available license (serial number) will be selected and licensing details transmitted to the Client – the connection bar changes from orange to green.



Licensing is now complete for this Client, indicated by the licenses status no longer being displayed in the lower frame.

From this point onwards the WatchGuard Mobile VPN Client is fully licensed and can establish VPN connections as required. No further activity is required in connection with licensing UNLESS there is an outage at the Mobile VPN License Server – see section 4.4.

NOTE: If an attempt is made to license a Client when all the licenses in a bundle have been used, then the message "Licensing operation failed" will be displayed and logged.

NOTE: In steps ii. & iii. above, if a VPN connection is established and the onwards connection to the MVLS is established immediately, the connection bar will only flash orange briefly before switching to green.

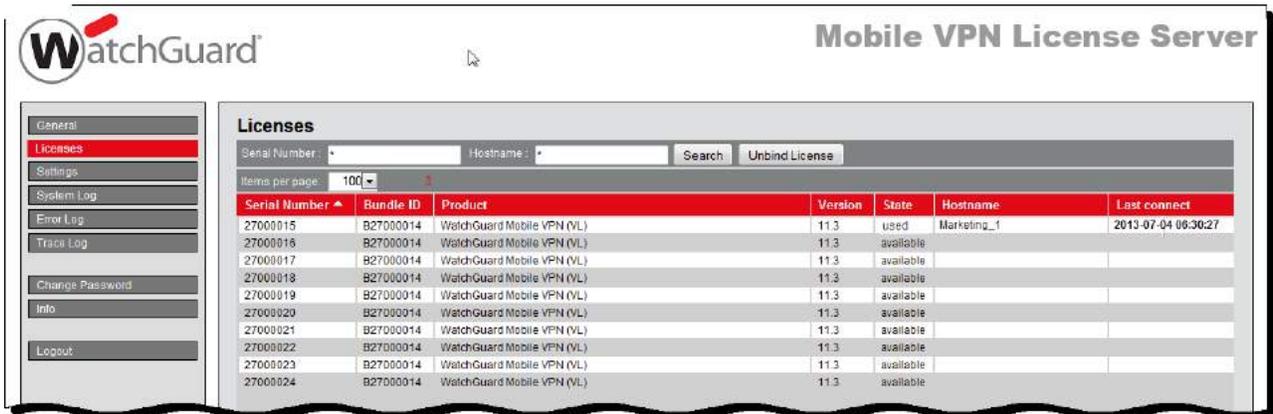
NOTE: In step ii. above, if a VPN connection is established but the onwards connection to the MVLS cannot be established, the connection bar will remain orange. Check that the MVLS is reachable from the VPN.

4.3. Client License States and Transferring Licenses between Clients License Bind and Unbind

In certain circumstances it may be necessary to transfer a license from one specific Secure VPN Client to another. This section describes the steps required to unbind and bind licenses and hence achieve the required license portability.

Detailed Procedure:

When Clients have been licensed and the system is running as normal, the "License" display at the MVLS console will look similar to the figure below:



License can have the following statuses:

"used"

If a Client has used a License (Client's hostname listed in "hostname" column)

"available"

If the license is still available

A Client (hostname) with a license status "used" can be unbound from a license/serial number by selecting the license and pressing "Unbind License" – that license/serial number will then show "available".

When a license/serial number has status "available", the [Client licensing procedures](#) described in section 4 can be used to license any un-licensed Client.

4.4. Adding Additional License Bundles

Use the procedures in step [4.1 b](#)) onwards, to add additional bundles to the MVLS's database. Screen images below illustrate how that additional information is displayed and can be sorted.

General
Licensee: MyKomypany, MyStreet 44, MyTown, 12345 CA, USA

The licenses purchased in a bundle must first be downloaded from the NCP Activation Server. An Initialization file will then be generated on this WatchGuard Mobile VPN License Server (VLS) and must be distributed to all Clients to be licensed. Using the initialization file, each Client establishes a connection (via the VPN) to this VLS and if a license is available, uses it to license the Client; the license serial number becomes bound to that Client. No further Clients can be licensed when each license in the bundle has been bound to a Client.

[Download Licenses](#)

Warning: It is highly recommended that the WatchGuard Mobile VPN License Server's configuration folder (C:\Program Files\Watchguard\Mobile VPN License Server\config) is included in the daily backup routine. In the event that the contents of this folder are lost and a backup is not available, all the corresponding Clients must be re-licensed. The initialization file that has already been distributed will be void; a replacement will have to be generated, distributed to the Clients and used for re-licensing.

Bundles

Bundle ID	State	Product	Version	No. of licenses	in use	not used	Initialization File	Info
B2700014	valid	WatchGuard Mobile VPN (VL)	11.3	10	0	10	Download	Info
B2700026	valid	WatchGuard Mobile VPN Mac OS (VL)	2.0	10	0	10	Download	Info
B2700041	valid	WatchGuard Mobile VPN (VL)	11.3	2	0	2	Download	Info

[Merge Bundles](#)

NOTE: All serial numbers that are associated with bundles downloaded to this MVLS are displayed in the "Licenses" screen. This list can be sorted by clicking on the header bar of the corresponding column.

Licenses

Serial Number: [] Hostname: [] [Search](#) [Unbind License](#)

Items per page: 100

Serial Number	Bundle ID	Product	Version	State	Hostname	Last connect
27900015	B2700014	WatchGuard Mobile VPN (VL)	11.3	available		
27900016	B2700014	WatchGuard Mobile VPN (VL)	11.3	available		
27900017	B2700014	WatchGuard Mobile VPN (VL)	11.3	available		
27900018	B2700014	WatchGuard Mobile VPN (VL)	11.3	available		
27900019	B2700014	WatchGuard Mobile VPN (VL)	11.3	available		
27900020	B2700014	WatchGuard Mobile VPN (VL)	11.3	available		
27900021	B2700014	WatchGuard Mobile VPN (VL)	11.3	available		
27900022	B2700014	WatchGuard Mobile VPN (VL)	11.3	available		
27900023	B2700014	WatchGuard Mobile VPN (VL)	11.3	available		
27900024	B2700014	WatchGuard Mobile VPN (VL)	11.3	available		
27900027	B2700026	WatchGuard Mobile VPN Mac OS (VL)	2.0	available		
27900028	B2700026	WatchGuard Mobile VPN Mac OS (VL)	2.0	available		
27900029	B2700026	WatchGuard Mobile VPN Mac OS (VL)	2.0	available		
27900030	B2700026	WatchGuard Mobile VPN Mac OS (VL)	2.0	available		
27900031	B2700026	WatchGuard Mobile VPN Mac OS (VL)	2.0	available		
27900032	B2700026	WatchGuard Mobile VPN Mac OS (VL)	2.0	available		
27900033	B2700026	WatchGuard Mobile VPN Mac OS (VL)	2.0	available		
27900034	B2700026	WatchGuard Mobile VPN Mac OS (VL)	2.0	available		
27900035	B2700026	WatchGuard Mobile VPN Mac OS (VL)	2.0	available		
27900036	B2700026	WatchGuard Mobile VPN Mac OS (VL)	2.0	available		
27900042	B2700041	WatchGuard Mobile VPN (VL)	11.3	available		
27900043	B2700041	WatchGuard Mobile VPN (VL)	11.3	available		
27900054	B2700053	WatchGuard Mobile VPN Mac OS (VL)	2.0	available		

The license(s) purchased can now be merged, if required - see [Merging License Bundles](#).

WatchGuard Mobile VPN License Server (MVLS)

Using an MVLS to manage Mobile VPN Client licenses

a) Bundle ID State

The Bundle ID "State" column always displays the current state of an individual Bundle ID. State can be one of the following values:

State	Meaning
valid	bundle has been validated and activated by the NCP Activation Server: this is the normal, operating state.
revoked	bundle has been revoked by NCP and should be deleted: contact WatchGuard for further details.
offline	bundle is no longer registered at the NCP Activation Server: contact NCP for further details.

b) Bundle ID Info

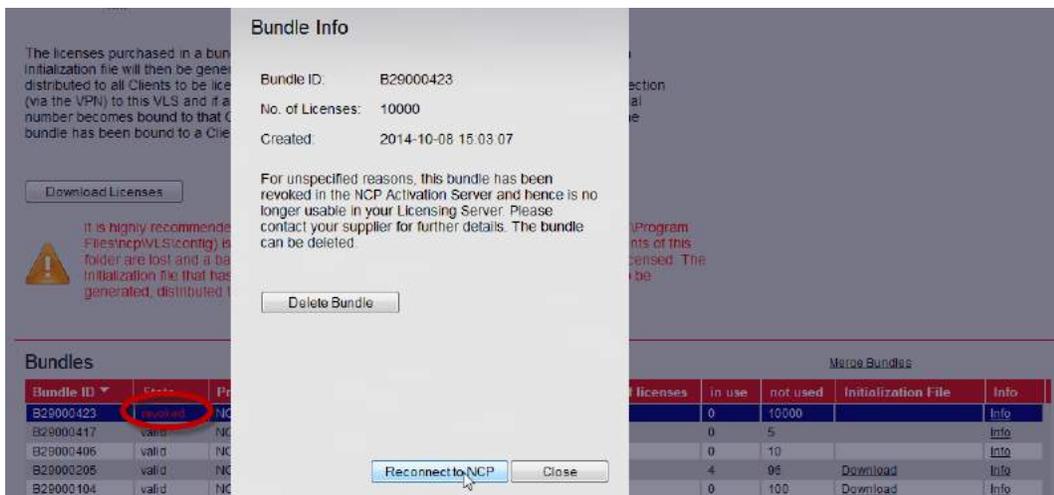
Use the respective Bundle ID "Info" link to open a dialog for:

- reconnecting the Bundle ID with the NCP Activation Server,
- creating a new Initialization File for the bundle,
- deleting a revoked Bundle ID.

c) Reconnect to NCP button and "revoked" Bundles

A license bundle, previously "revoked" due to various circumstances, may need to be made "valid" again; this will inevitably be being done under the guidance of NCP support.

In such a situation various timers within the MVLS may delay the setting of the "valid" flag.



The screenshot shows the 'Bundle Info' dialog for Bundle ID B29000423. The dialog indicates that the bundle has been revoked and is no longer usable. A 'Reconnect to NCP' button is visible at the bottom of the dialog. The background shows a table of bundles with columns for Bundle ID, State, and Actions.

Bundle ID	State	Pr
B29000423	revoked	NC
B29000417	valid	NC
B29000406	valid	NC
B29000206	valid	NC
B29000104	valid	NC

To reduce the delay, use the "Reconnect to NCP" button in the Bundle Info dialog.

Providing the license has been suitably reset by WatchGuard, the "valid" flag will then be re-displayed after 2-3 minutes.

Using an MVLS to manage Mobile VPN Client licenses

4.5. Merging License Bundles for a specific product - Merge Bundles

Use the Merge Bundles feature to merge a new license bundle, purchased and downloaded from NCP (see 4.4 above) after the original Initialization File was created, with an existing bundle (or bundles). The benefit of the feature is that the original Initialization File can continue to be used to distribute those licenses that have been subsequently purchased; one Initialization File is used to license Clients from a number of different bundles, even if those bundles were purchased after the Initialization File was created.

Restrictions when using Merge Bundles:

- only license bundles for a specific product and a specific software version number can be merged together,
- if multiple software versions of a specific product are in use, a merged bundle of licenses must be created for each specific product / software version number set, and
- only one merged bundle (i.e. one Initialization File) can be created per product/software version set.

Detailed Procedure:

The images below illustrate a real-life situation and are logically consistent throughout the procedure described.

a) On the General / Bundles page, select the "Merge Bundles" link

Bundles								Merge Bundles	
Bundle ID	State	Product	Version	No. of licenses	in use	not used	Initialization File	Info	
B27000014	valid	WatchGuard Mobile VPN (VL)	11.3	10	0	10	Download	Info	
B27000026	valid	WatchGuard Mobile VPN Mac OS (VL)	2.0	10	0	10	Download	Info	
B27000041	valid	WatchGuard Mobile VPN (VL)	11.3	2	0	2	Download	Info	
B27000053	valid	WatchGuard Mobile VPN Mac OS (VL)	2.0	5	0	5	Download	Info	

b) On the Merge Bundles page, decide which bundle is to be the "top-level" bundle, i.e. the bundle whose Initialization File is to be used with the merged bundle, and press its "Merge" link.



Mobile VPN License Server

General

[Licenses](#)

[Settings](#)

[System Log](#)

[Error Log](#)

[Trace Log](#)

[Change Password](#)

[Info](#)

[Logout](#)

Merge Bundles

Bundles purchased over time can be merged together, enabling a single Initialization File, created when the first bundle was purchased, to continue to be used to distribute licenses from subsequently purchased bundles. The individual bundles of licenses for the same product and version are indicated graphically below. Colors are only used to differentiate between product/version combinations and are allocated top down across the whole list. To merge one bundle with another bundle (or bundles):

- 1) Decide which bundle has the Initialization File to be used with a set of merged bundles - the Top-Level bundle.
- 2) Press the "Merge" link in that bundle and follow the instructions on the next screen. Repeat to merge each of three or more bundles.

Use the "Unmerge" link to unmerge a bundle.

Unmerged Bundles:

WatchGuard Mobile VPN (VL) 11.3
B27000014 Number of Licenses: 10

[Merge](#)

WatchGuard Mobile VPN (VL) 11.3
B27000041 Number of Licenses: 2

[Merge](#)

WatchGuard Mobile VPN Mac OS (VL) 2.0
B27000026 Number of Licenses: 10

[Merge](#)

WatchGuard Mobile VPN Mac OS (VL) 2.0
B27000053 Number of Licenses: 5

[Merge](#)

Explanation:

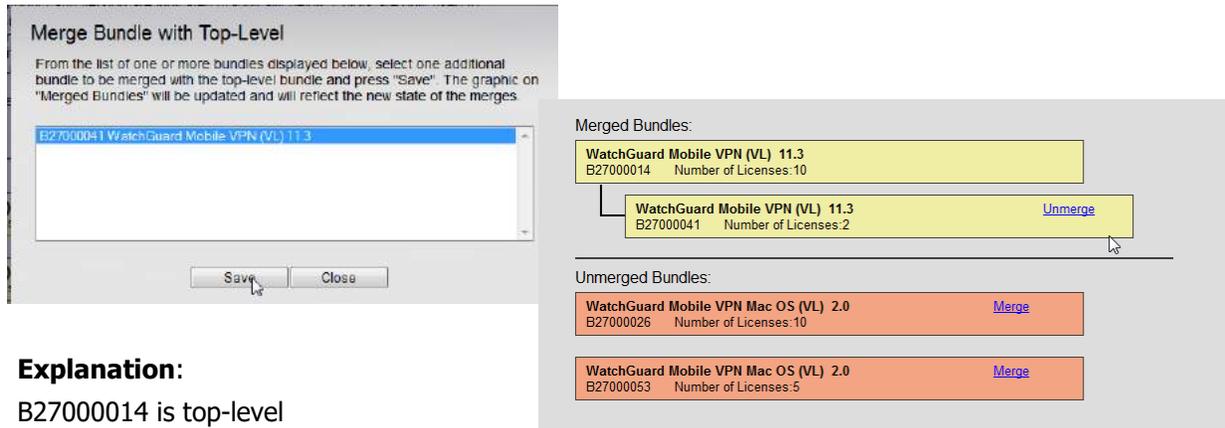
B27000014 will be the top-level bundle

B27000041 will be merged with B29000205

WatchGuard Mobile VPN License Server (MVLS)

Using an MVLS to manage Mobile VPN Client licenses

- c) In the list displayed, select the product bundle to be merged with the top-level



Merge Bundle with Top-Level

From the list of one or more bundles displayed below, select one additional bundle to be merged with the top-level bundle and press "Save". The graphic on "Merged Bundles" will be updated and will reflect the new state of the merges

B27000041 WatchGuard Mobile VPN (VL) 11.3

Save Close

Merged Bundles:

- WatchGuard Mobile VPN (VL) 11.3 B27000014 Number of Licenses:10
- WatchGuard Mobile VPN (VL) 11.3 B27000041 Number of Licenses:2 [Unmerge](#)

Unmerged Bundles:

- WatchGuard Mobile VPN Mac OS (VL) 2.0 B27000026 Number of Licenses:10 [Merge](#)
- WatchGuard Mobile VPN Mac OS (VL) 2.0 B27000053 Number of Licenses:5 [Merge](#)

Explanation:

B27000014 is top-level

B27000041 is merged and can use the same Initialization File. **Note:** a bundle can be subsequently unmerged by clicking the "Unmerge" link

B27000026 and 53 can be merged together as a separate merged bundle.

- d) repeat steps b) and then c) for each additional bundle to merged with the top-level bundle.

Note:

- at this stage, the top-level bundle will be shown in the Merged Bundles part of the diagram, and
- a "Merge" link is displayed in the top-level only when a suitable bundle is available for merging; no "Merge" link is displayed in B27000014 as there are no more bundles that can be merged with B27000014.

- e) when bundles have been merged, the General/Bundles screen only shows a Download link (for the Initialization File) against the top-level bundle:

Bundles							Merge Bundles		
Bundle ID	State	Product ^	Version	No. of licenses	in use	not used	Initialization File	Info	
B27000014	valid	WatchGuard Mobile VPN (VL)	11.3	10	0	10	Download	Info	
B27000041	valid	WatchGuard Mobile VPN (VL)	11.3	2	0			Info	
B27000026	valid	WatchGuard Mobile VPN Mac OS (VL)	2.0	10	0	10	Download	Info	
B27000053	valid	WatchGuard Mobile VPN Mac OS (VL)	2.0	5	0	5	Download	Info	

Using an MVLS to manage Mobile VPN Client licenses

4.6. License Activation when Updating to a Newer Version of WatchGuard Mobile VPN

When a WatchGuard Mobile VPN Client must be updated to a new version - for example, from release 11.3x build yyy to release 11.40 build yyy - then the following steps must be followed in order to ensure the minimum of user disruption and, in particular, that the firewall on the WatchGuard Mobile VPN, if already turned on by configuration options, is not inadvertently turned off.

- 1) Download the new bundle of licenses from the NCP Activation Server and generate a new Initialization File - follow procedures in sections 4.1. 2) and 4.1. 6)

Important: before generating the Initialization File, ensure that the MVLS configuration details - IP address, proxy IP address/port number - reflect the actual state of the MVLS machine.

After these two steps have been carried out, the original license serial numbers from the original license bundle will no longer be available, attempts by Mobile VPN Clients to validate their licenses will fail, and the Mobile VPN Clients will be returned to the "Test License" / "Ready for Licensing" state. In this state, all features except VPN tunnel establishment are disabled, meaning that the firewall is also disabled.

In order to minimize interruptions to user's work and reduce the risk of exposure to network based viruses etc., the next steps must be carried out without delay.

- 2) License the WatchGuard Mobile VPN Client Software - follow procedure in section 4.2. 3)
- 3) IMMEDIATELY establish a VPN tunnel to the WatchGuard VPN gateway.

When the VPN tunnel has been established, the Mobile VPN Client will automatically carry out the license activation process, thereby enabling all features of the new software version, including the firewall if it was previously enabled.

Using an MVLS to manage Mobile VPN Client licenses

4.7. Mobile VPN License Server Outages, and associated Client Recovery

Unless fundamental changes were made to the Mobile VPN License Server configuration during recovery from a machine or OS outage, most Clients will be able to continue to use the VPN without interruption. The only Clients affected by a MVLS outage will be those which were licensed since the last backup was performed (i.e. the backup from which recovery was/will be performed).

Recovery procedures for those specific Clients is to simply use the existing Initialization File to re-license the Client.

Failure to re-license one of those such Clients will mean that the user of that Client will no longer be able to use the VPN – VPN connection establishment will fail.

WatchGuard recommends that, in the case of a MVLS outage, a general notice be issued to all VPN users along the following lines:

LICENSING SERVER OUTAGE

- Licensing Services from the Local Licensing Server have been interrupted.
- These services will be resumed ASAP.
- If your PC/workstation/smartphone uses a WatchGuard Mobile VPN Client which was installed AFTER “date and time of last backup”, you will need to re-license your Client when the Licensing Services are resumed.
- You will be notified when Licensing Services have been resumed.
- Please contact the license administrator - details displayed in the Licensing section of the NCP Client Monitor - if you require further assistance.

Using an MVLS to manage Mobile VPN Client licenses

4.8. Changing the MVLS Machine's IP Address - and Licensing Implications

WatchGuard strongly recommends that, when designing the network in which the MVLS will be located, the MVLS machine's IP address allocation be performed dynamically using DNS; this obviates the need for future changes such as described below.

If a change to the MVLS machine's IP address is unavoidable, then the Initialization File generated using the old IP address becomes invalid and all Clients already licensed under the old IP address must be relicensed - there are no exceptions to this rule.

Use the following procedure to change the IP address and relicense the Clients affected by the change.

4.8.1. Change the MVLS machine's IP address

- 1) Change the machine's IP address using the appropriate functions in the underlying Windows operating system.
- 2) Open the "Settings" page and select the required IP address from the pulldown list. The list will display addresses for all adapters configured in the machine; it is important that the correct address be selected.

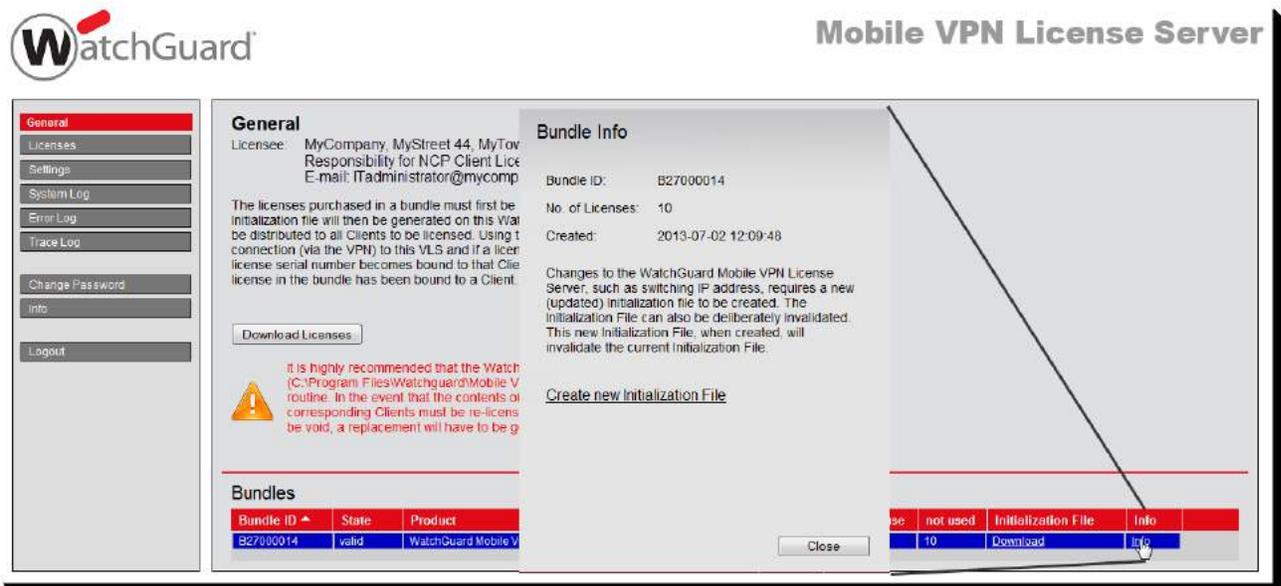


3) Enter Proxy details as necessary

and press "Save".

4.8.2. Generate a new Initialization File

- 1) Open the "General" page, here each license entry (line) contains an "Info" tab:
- 2) Click on the "Info" link against the licenses to be reapplied; this opens the "Bundle Info" window:



- 3) Click on "Create new Initialization File"

Using an MVLS to manage Mobile VPN Client licenses

- 4) A message is displayed in the next window, indicating that the Initialization File has been regenerated and pointing to the downloadable file. Download the file (or download it as part of the relicensing procedure - see below) and close the window.

4.8.3. Relicense Affected Clients

As soon as the MVLS machine's IP address is reconfigured (step 4.5.1 above), all attempts by Clients to connect to the MVLS and validate their license will fail. Eventually attempts to establish a VPN tunnel will also fail and the Mobile VPN Client software will no longer be useable.

To avoid prolonged delay in bringing the Clients back online, the Initialization File regenerated in 4.5.2 must now be used immediately to relicense all the affected Clients - use the procedure described in section 4.2.

Using an MVLS to manage Mobile VPN Client licenses

5. Clients - Versions supported by this MVLS version

The following Mobile VPN Client versions are supported by this version of a MVLS:

WatchGuard Mobile VPN (Windows variant) - Version 11.32 and higher

WatchGuard Mobile VPN (Mac OS X variant) - Version 2.05 and higher

6. Document Revision Status

Revision status is displayed on front page of document.

Revision	Changes
July 2013	First issue
October 2014	S/W Version 2.00 release Merge Bundles added Mac OS X Client installation added Various section order and layout changes to improve logical flow
September 2019	Added hostname of NCP Activation Server (actsrv1.ncp.de)