QuickStart Guide

high security remote access

NCP Volume License Server (VLS)

Using a VLS to manage licenses for Secure Android Client Volume Edition or Secure Client – Juniper Edition

As of August 2013
NCP Volume License Server: version 1.03

Network
Communications
Products engineering

USA:

NCP engineering, Inc.
444 Castro Street, Suite 711
Mountain View, CA 94041
Tel.: +1 (650) 316-6273
Fax: +1 (650) 251-4155

Europe:

NCP engineering GmbH
Dombuehler Str. 2
D-90449 Nuremberg
Tel.: +49 (911) 9968-0
Fax: +49 (911) 9968-299

Internet

http://www.ncp-e.com

Email

info@ncp-e.com

Support

NCP offers support for all international users by means of Fax and Email.

Email Addresses

helpdesk@ncp-e.com (English)
support@ncp-e.com (German)

Fax

+1 (650) 251-4155 (USA)
+49 (911) 9968-458 (Europe)

When submitting a support request, please include the following information:

- exact product name
- serial number
- version number
- an accurate description of your problem
- any error message(s)

Copyright

Contents

1. Introduction

This manual describes:

- the management and distribution of licenses to large numbers of NCP Secure Clients,
  either
  NCP Secure Client – Juniper Edition
  or
  NCP Secure Android Client Volume Edition (a variant of the NCP Android Secure Managed Client).
- the functionality provided by NCP's Volume License Server (VLS) in combination with those Secure Clients, and
- the procedures that must be undertaken by Virtual Private Network (VPN) administrators to manage the Secure Clients and their associated licenses.

2. Overview

The NCP Volume License Server can be used to manage the distribution of licenses for the NCP Secure Clients listed above. Designed to simplify the management of software licenses for a large number of NCP Secure Clients that make use of a VPN infrastructure, the VLS maintains an inventory of licenses that have been purchased from NCP, 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 VLS are guaranteed to be secure against eavesdropping, tampering or theft.

2.1. NCP Secure Client product licenses

Licenses to be managed via a Volume License Server are purchased from NCP 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 NCP in either paper or electronic form.
- All licenses represented by a bundle are associated with a specific NCP Secure Client product, **either** a specific NCP Secure Client – Juniper Edition product and software version
  or
  a specific NCP Secure Android Client Volume Edition product and software version.

  Juniper Client licenses cannot be used to license Android Clients and vice versa.
- The information making up a bundle is downloaded from NCP's Activation Server in electronic form. During an initialization transaction between the Volume 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 an NCP Secure Client for an unspecified period of time.
- The serial number is bound to a specific NCP Secure Client by running
  a) the Software Activation Wizard at a Secure Client – Juniper Edition machine,
  or
  b) the IMPORT LICENCE procedure at an NCP Secure Android Client Volume Edition device.
- 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.

2.2. Licensing NCP Secure Clients using the VLS

Licenses purchased for use with a Volume License Server are distributed to each NCP Secure Client as follows:

- The licensing application – the Volume License Server - runs on a Microsoft Windows based server. At all times, the VLS 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 Volume 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 VLS.

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

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

- The VLS 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 VLS) is secured via the Secure Socket Layer (SSL) protocol.

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

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

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

  NOTE: The IP address (or fully qualified domain name if DNS is in use) of the VLS is one of the items stored in this file. If, for any reason, the IP Address of the VLS changes in the future, all Clients licensed via this VLS (i.e. with the original IP Address) will no longer be able to communicate with the VLS 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 VLS IP Address is liable to change in the future, you are advised to allocate a Fully Qualified Domain Name to the VLS and use DNS to distribute the IP address to Clients and VPN gateways.

  See also

  section 4.4 - VLS Server Outages, Backups and Recovery
  and
  section 4.5 - Changing the VLS Machine's IP Address - and Licensing Implication

- 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 NCP Secure Client that can connect to the organization's VPN gateway.

- At each Secure Client machine
  - the appropriate NCP Secure 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 VLS should ideally be carried out during the standard 30 day (Juniper) or 10 day (Android) 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 Secure Client uses information in the Initialization File, in combination with information from the VLS, to bind a serial number to that Secure 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 Secure 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 Volume License Server. The Client is only fully licensed when this license details exchange process has been successfully completed.
- On licensing the Client, the VLS database is updated with the following details:
  - NCP Secure 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.
- 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 VLS, each Client must periodically check its status at the VLS, 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.

2.3. VLS 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 VLS.

2.3.1. Recommended Backup and Restore Procedure.

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

- If, for any reason, the VLS fails (system failure causing the VLS 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 VLS database will have been lost.

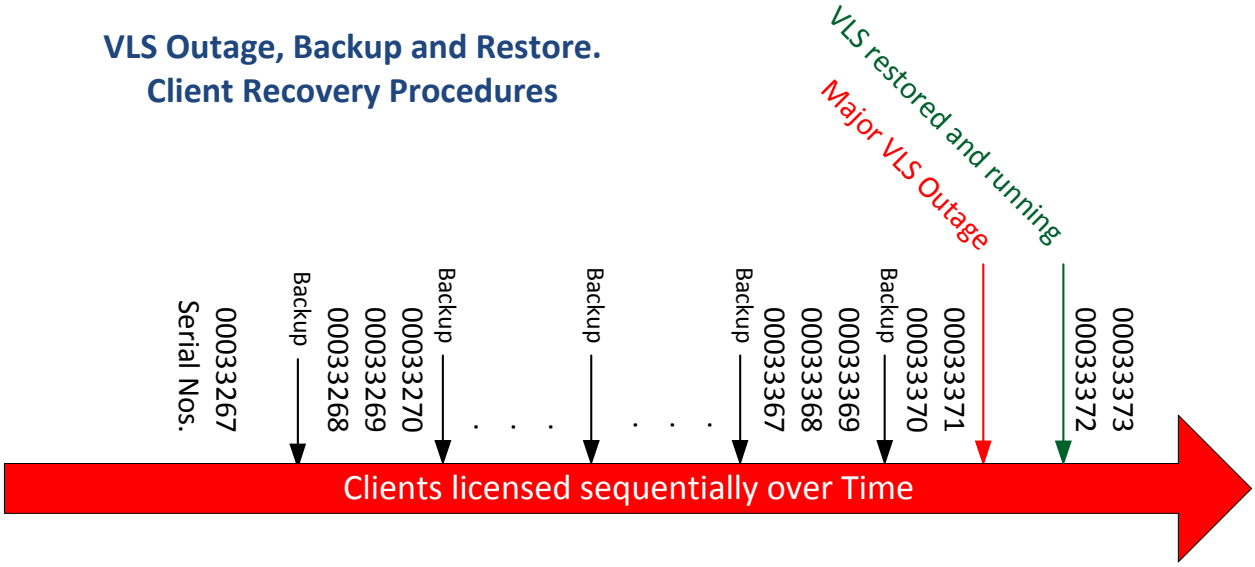
Due to this potential for loss of data it is recommended that a backup of the VLS configuration folder (default location):

C:\Program Files\ncp\VLS\config

be performed on a regular basis.

If a VLS outage occurs which requires a recovery:

- reinstall or recover the OS using standard procedures
- reinstall the Volume License Server software – see section 4
- copy the latest backup of the configuration VLS folder to:
  default location C:\Program Files\ncp\VLS\config\
- The figure on the next page illustrates details of any Client recovery procedures that might be necessary.



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

After the VLS 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 VLS 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 VLS web interface Licenses display
  - user support procedures should signal the VLS 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 section 4.4).
- 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.

3. Installing and Operating a Volume License Server

3.1. Installation Prerequisites

Volume License Server machine[1]	**Hardware**: Any commercially available Intel X86 based machine. Backup Device: backup device with sufficient capacity to hold regular system backups – see section 2. **Operating System**: Microsoft Windows (32 or 64 bit) Server operating systems: MS Windows Server 2003 or newer **OS Services to be started or stopped**: None specific to the VLS service
Network **Note: all IP routes must be available at all times**	**VPN Subnet**: Each Secure Client must be able to access the VLS via its VPN tunnel established to the VPN gateway. **Client to VLS IP access (Firewall port) - via VPN subnet**: Port 12503/TCP on the VLS machine must be accessible from each Client. This link is secured via an SSL tunnel between Client and VLS. **Internet**: An IP route between VLS and NCP Activation Server MUST be available to allow the VLS to periodically build an SSL VPN connection to the NCP Activation Server. An HTTPS proxy IP address can be configured at the VLS to enable this connection if necessary.
Administration Web Console	**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 VLS server machine if this has the necessary graphics support. **Browser to Server Authentication Certificates**: During VLS installation, a self-signed browser–server certificate is automatically generated. This is used to authenticate the web console browser with the VLS. **Web Console to VLS IP access (Firewall port)**: Port 20132/TCP on the VLS machine must be accessible from the web console machine.
NCP Secure Clients	**The following NCP Secure Clients can be licensed using a VLS**: NCP Secure Client – Juniper Edition version 9.25 and later NCP Secure Android Client Volume Edition version 2.32 build 018 and later

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

3.2. Installation

Ensure that the MS Windows OS is completely installed on what will become the VLS, 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 VLS. If the web console is to be run on the VLS machine, the web browser to be used must be defined as the default browser.

a) Install Volume License Server Software

- Download the VLS installation package from NCP 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 "NCP_VLS_Win3264_aaa_bbb.exe" file with administrator rights (RT mouse, run as administrator) to call the Installation Wizard.
  (aaa = version number, bbb = build number)

Press "Next" to display the standard NCP license terms for the VLS software

Press "Yes" to accept the license terms and display the final screen

- If the Administration Web Console browser is to be hosted on the VLS 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.

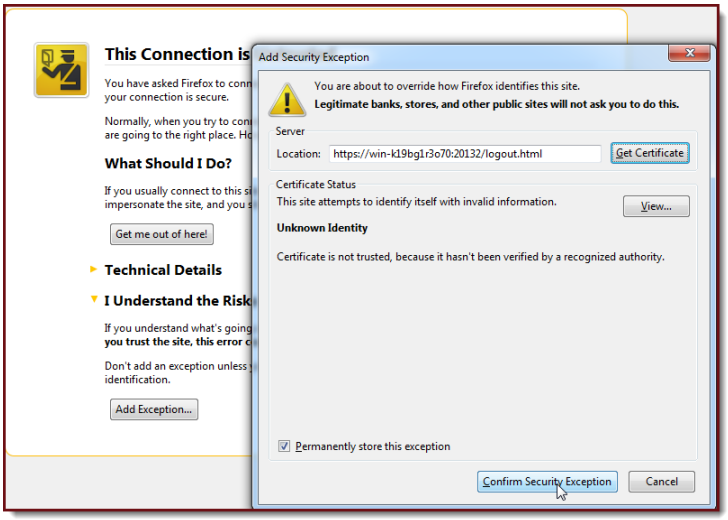
b) Call the VLS Administration Web Console

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 VLS

c) Web Browser <> Web Server Authentication

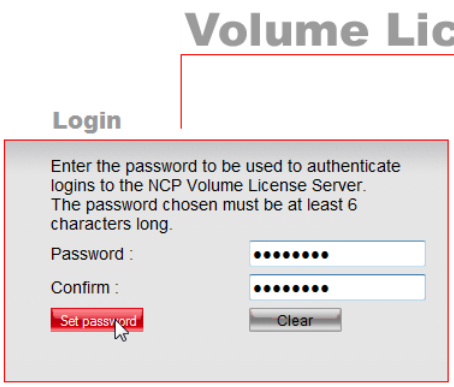
As an HTTPS URL has been entered, this invokes the HTTPS client <> server authentication process.



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

d) Define a VLS administrator password

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



Enter a suitable password and press "Set password"

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

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

3.3. Operating the VLS

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

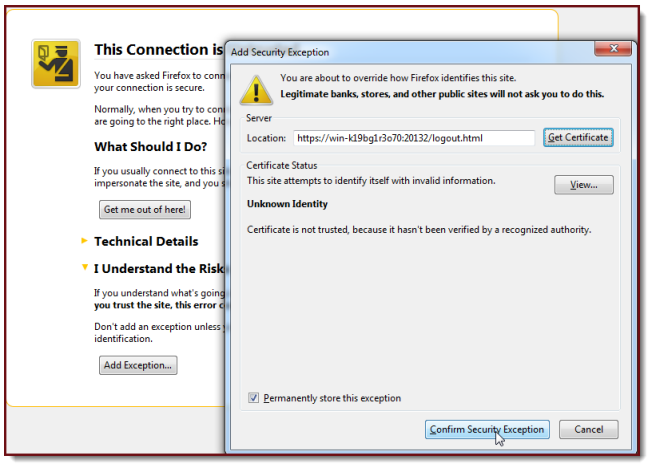
3.3.1. Starting and Stopping the VLS application/service

The VLS 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 VLS application/service.

3.3.2. To login to the VLS 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 VLS from this browser, the certificate download process must be carried out:



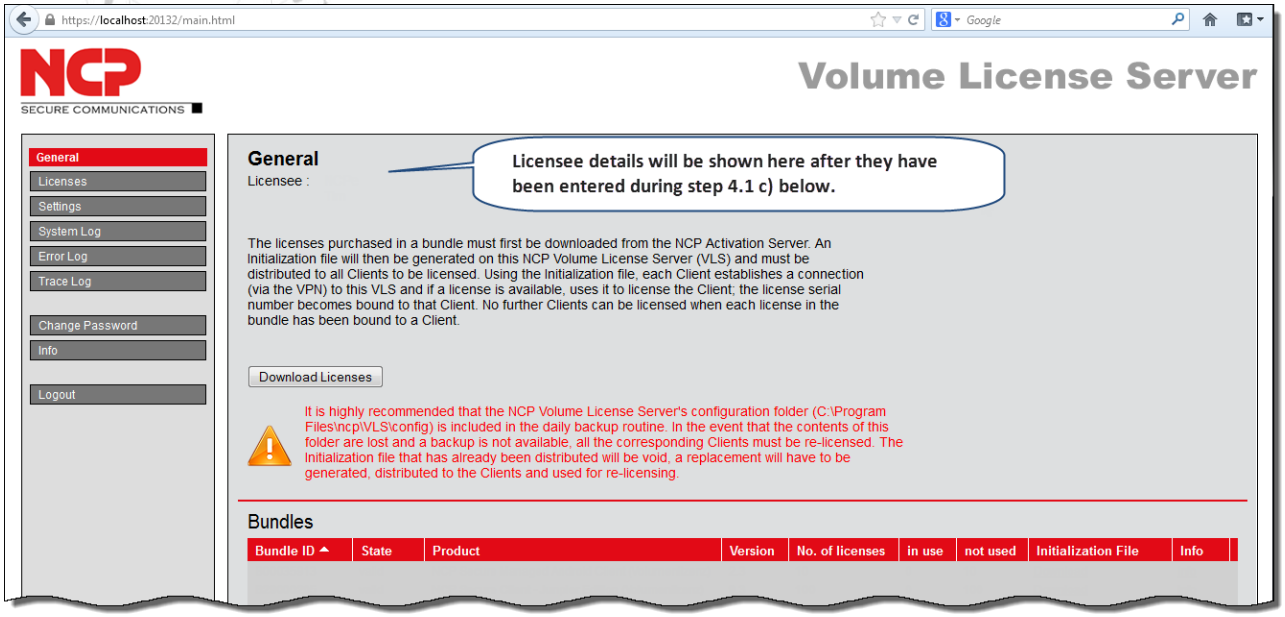
Get the certificate

and then

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

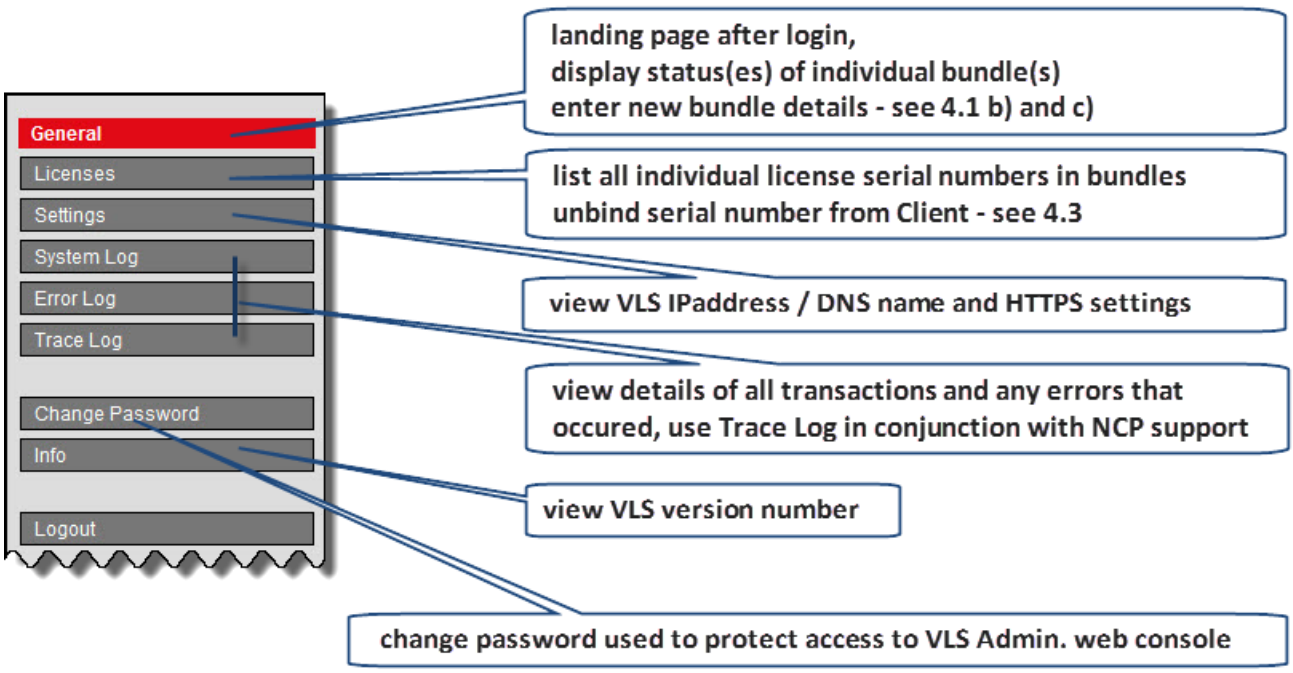
The Login screen is then automatically displayed.

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



3.3.3. Overview of VLS Administration Web Console Menu

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



4. Managing Licenses

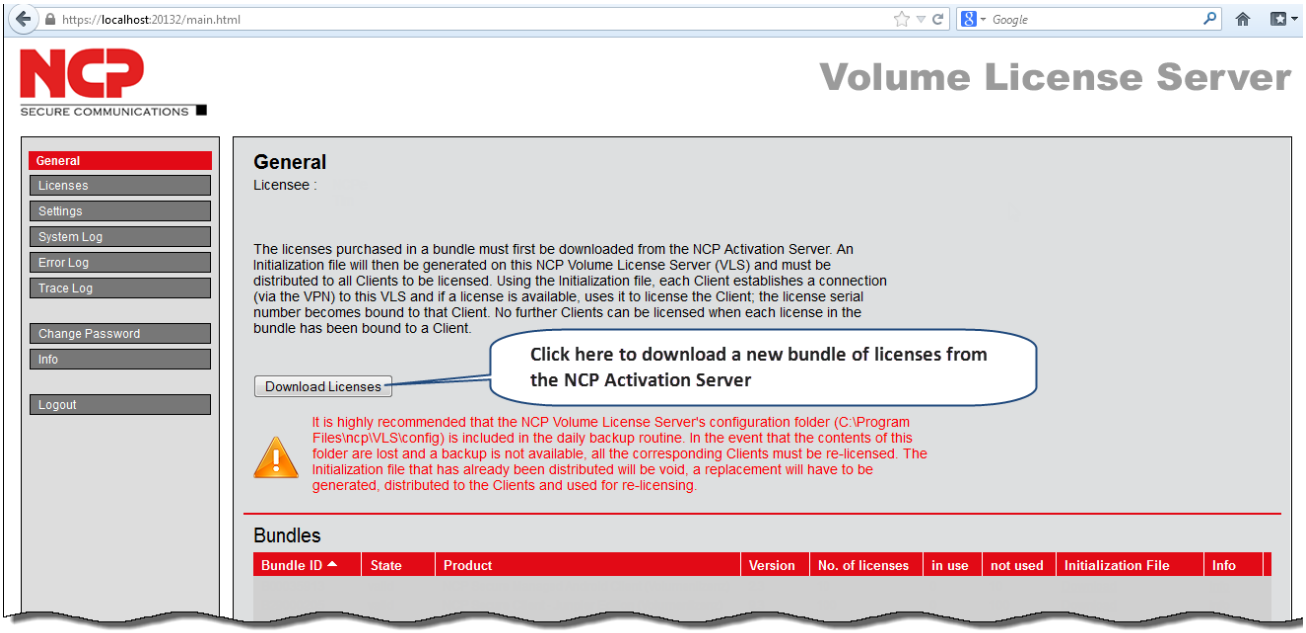
This section describes in detail how license bundles are downloaded to the Volume License Server and how Client licensing is performed

4.1. Setting up the VLS after Installation

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

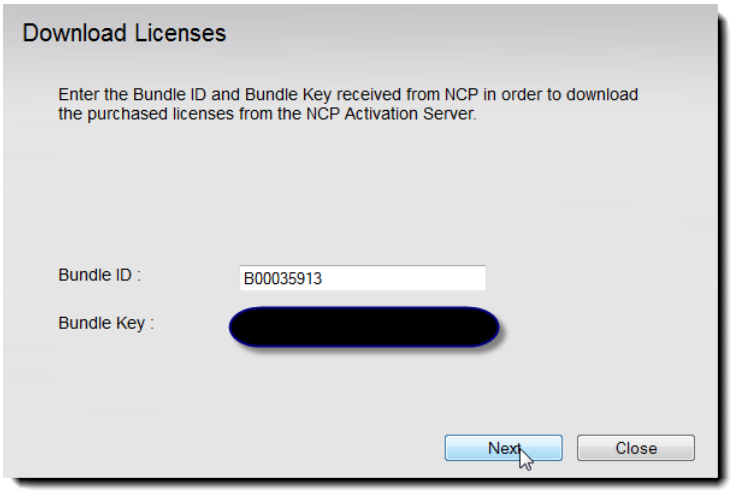
a) Login to the VLS Web Console

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



b) Enter Bundle Details

The "Download Licenses" screen is displayed:



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

Press "Next" to continue

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

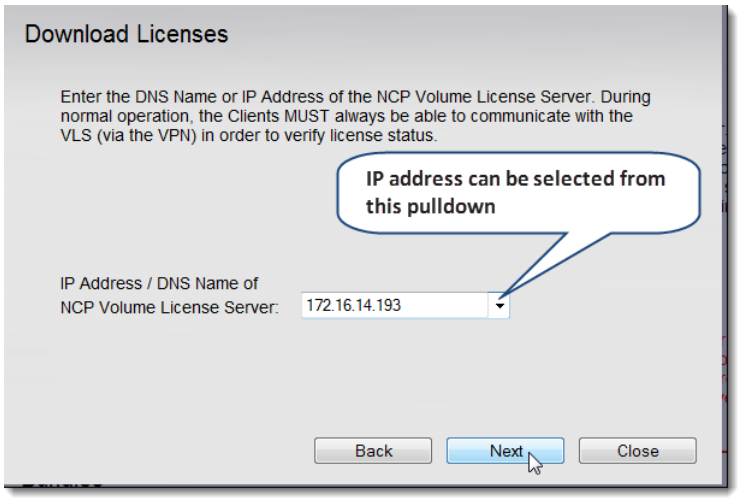
As this is the first bundle being entered into the VLS's database, you are now prompted to enter Licensee details. The 3 lines are free format and are displayed at each Client when it has been licensed.

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 VLS. If a DNS Name is to be used for the server it must be entered here.



NOTE: The IP addresses displayed in the pull-down are those that were active on the VLS machine when the VLS application was started.

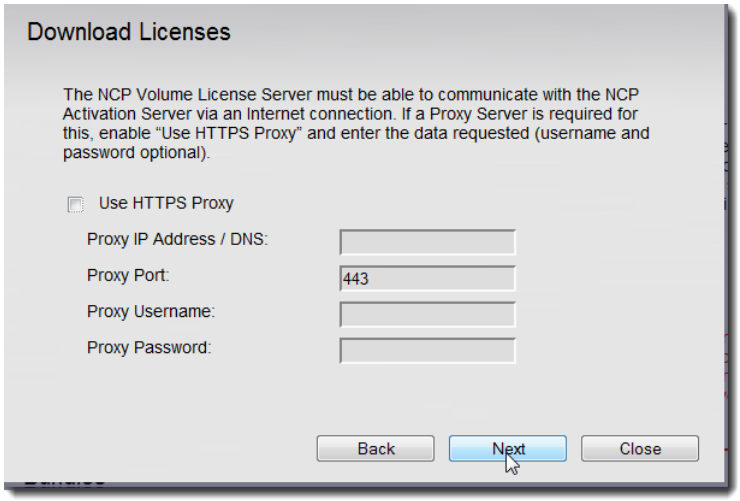
Adapters introduced to the machine after the VLS application was started will not show in this list.

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

NOTE: Changing the IP Address of the VLS machine at any point after it is configured here will cause all currently licensed Clients to become unlicensed – they would be unable to undertake the regular validation of their licenses against the VLS database. You are advised to contact NCP support if it becomes necessary to change the VLS IP Address once Clients have been licensed.

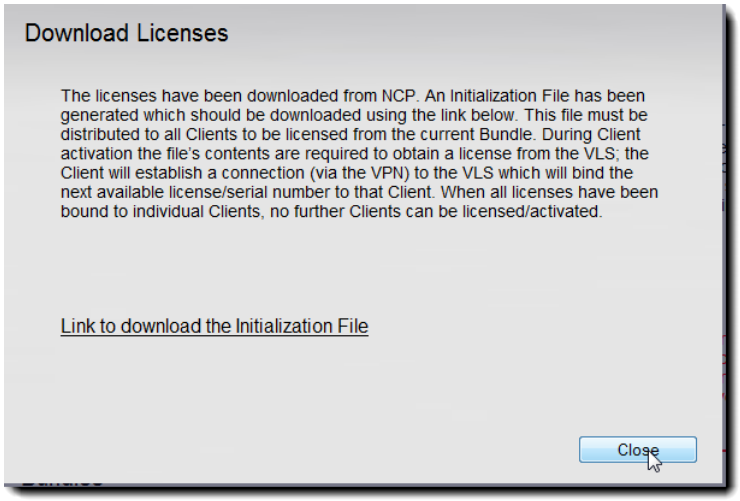
e) HTTPS Proxy to be used or not?

If an HTTPS proxy must be used to enable communications between the VLS 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 VLS establishes a connection to the NCP Activation Server and the license details associated with the bundle selected are downloaded to the VLS. The Initialization File is then generated and can be downloaded to any media (USB stick etc.) accessible via the web console machine.

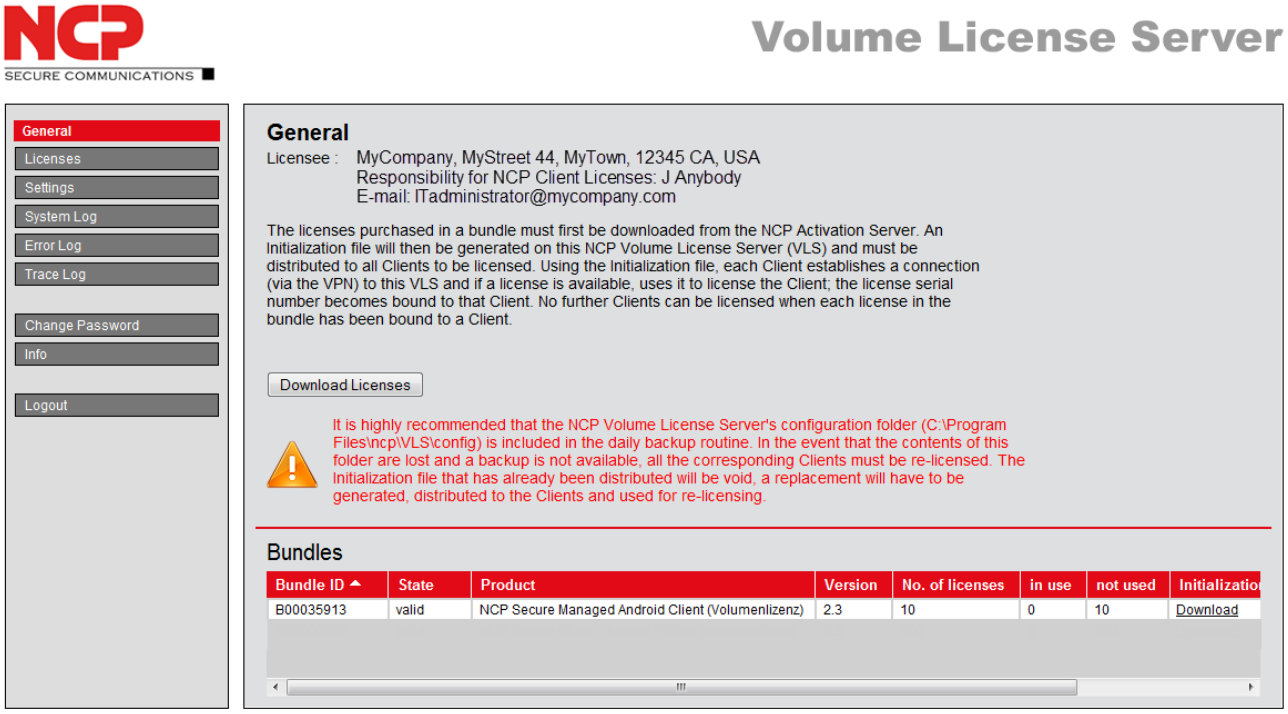


NOTE: If you wish to download the Initialization File immediately, click the link here and download the file (see details in Section 4.1 j) and press "Close",

otherwise just press "Close"

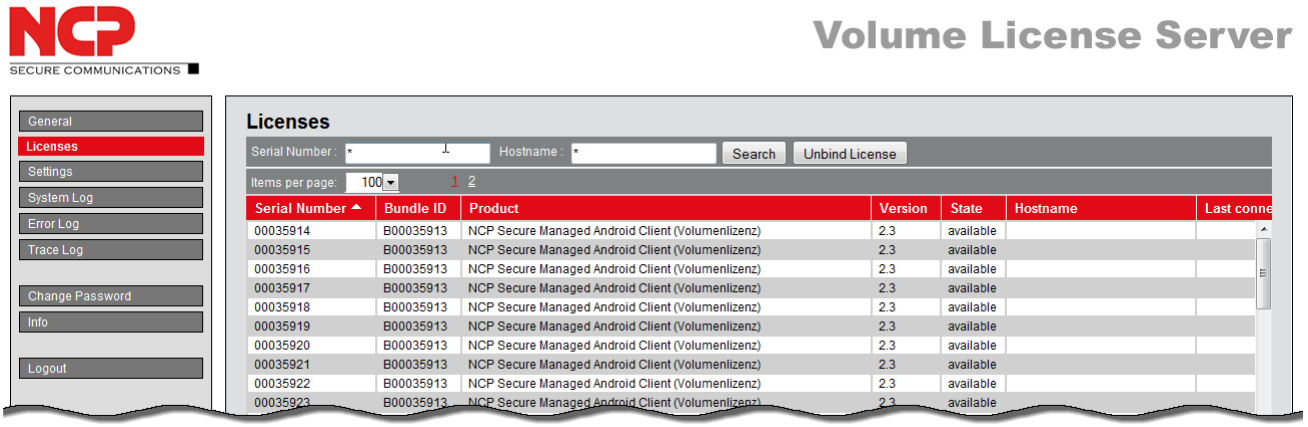
g) License Details now stored in VLS

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



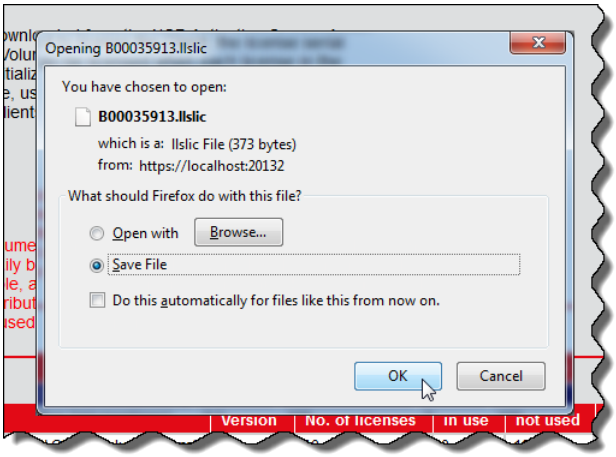
h) Displaying Bundle Details - Serial Numbers Used / Available etc.

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 VLS.



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:



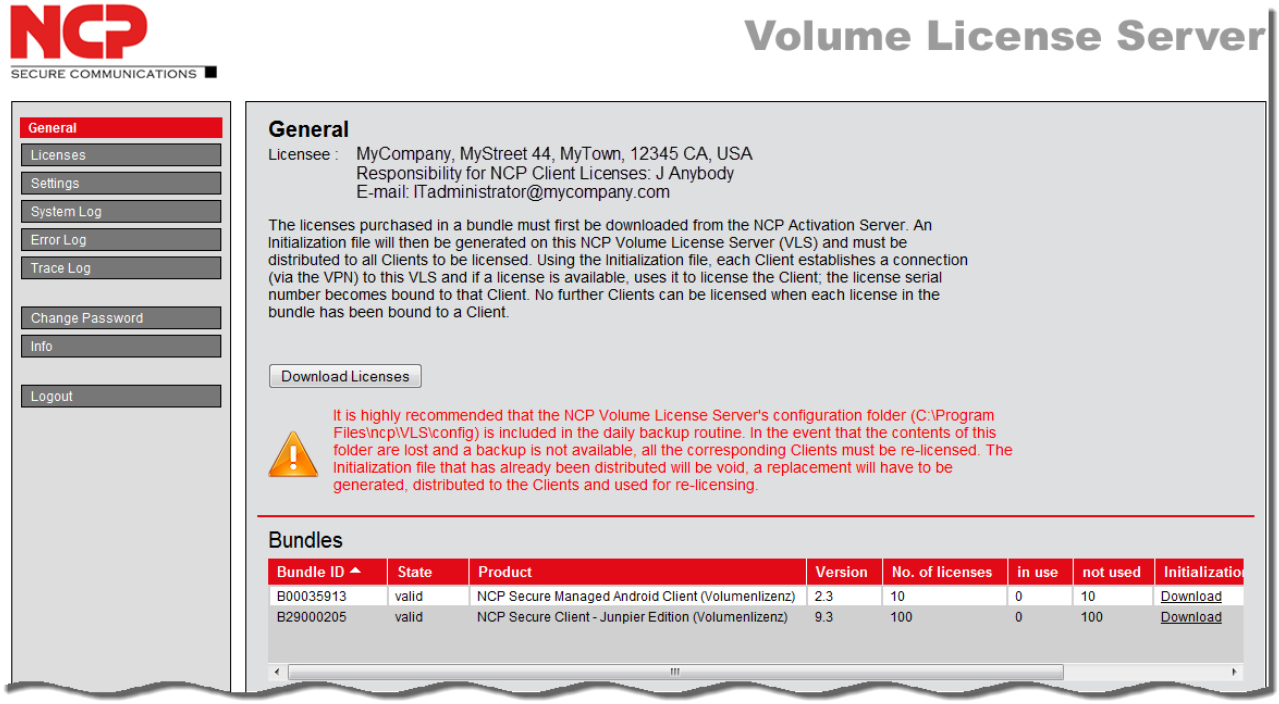
Select the "Download" link of the bundle Initialization File which you wish to create and press RT mouse.

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

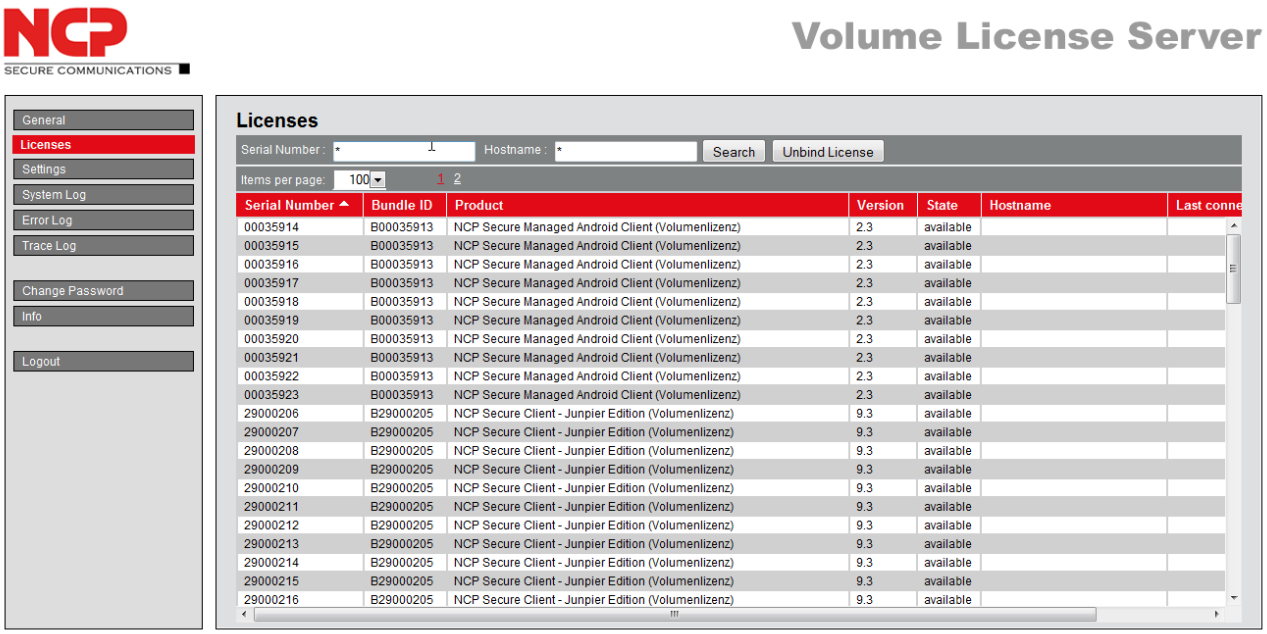
NOTE: This file can only be used to license Clients that correspond to the Product and Version Number defined in the original bundle.

j) Adding Additional Bundles

Use the procedures in steps b) and f) and g) to add additional bundles to the VLS's database. Screen images below illustrate how that additional information is displayed and can be sorted.



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



4.2. Licensing NCP Secure Clients

The Initialization File created in step 4.1 i) must be distributed to all those NCP Secure Clients to be licensed. 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 Secure Client being licensed.

4.2.1. Licensing an NCP Secure Client - Juniper Edition

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 Secure Client - Juniper Edition Software

- Install the Secure Client - Juniper Edition software using standard NCP installation procedures.
- Start the Client Monitor - this will make use of the 30 day free-use license delivered with the Client.
- Create a Connection Profile that establishes a connection to the corporate VPN gateway – this profile will used during the Juniper Client's licensing process to communicate with the VLS.

c) License the Secure Client - Juniper Edition Software

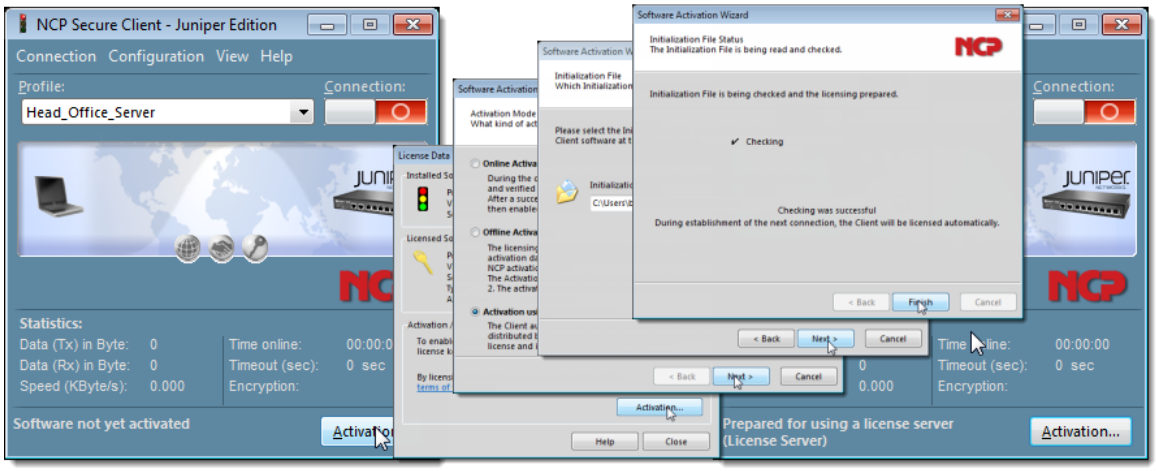
Licensing an individual Secure Client -Juniper Edition is a two step process as follows:

1. Import the Initialization File and run the software activation process

   There are two methods for importing the Initialization File,

   either:

   a. Use the Software Activation Wizard



   - 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

b. 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)\NCP\SecureClient)
   - 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.

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.

Regardless of which method is used, the activation status is displayed in the lower frame of the Client Monitor:

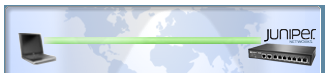
2. Complete the Client licensing by exchanging licensing details between Client and VLS via the Corporate VPN

   Establish a tunnel to the VPN gateway using the Connection Profile defined in step b) above. During the 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 Volume 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

   From this point onwards the Secure Client - Juniper Edition 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 Volume 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 VLS 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 VLS cannot be established, the connection bar will remain orange. Check that the VLS is reachable from the VPN.

4.2.2. Licensing an NCP Secure Android Client Volume Edition

a) Check IP Connection to VPN gateway

Once the OS on the Client machine has been installed, ensure it is connected to the IP communications network.

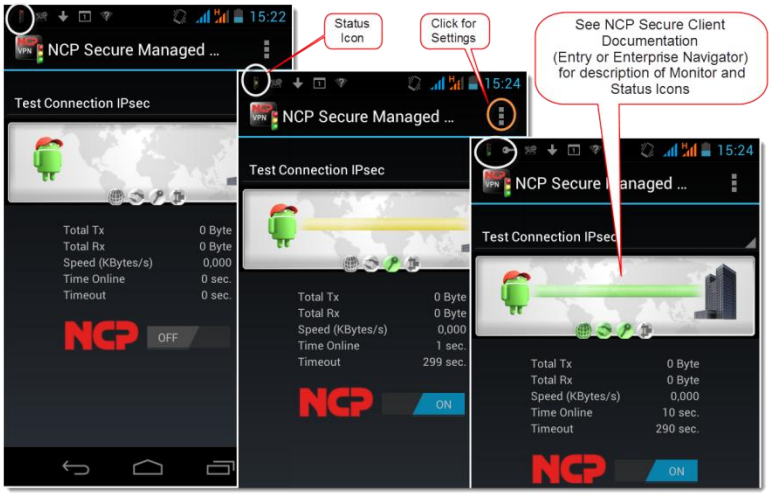
b) Install Client Software

- Install the Client software using standard NCP installation procedures.

- Start the Secure Client by clicking the app Icon

  this will make use of the 10 day free-use evaluation license delivered with the Client.

- Use the "Test Connection IPsec" Connection Profile to test that a tunnel can be successfully established to NCP's test VPN gateway.



- Create a Connection Profile that establishes a tunnel to the corporate VPN gateway – this profile will used by the Client's licensing process to communicate with the VLS.

c) License the Client Software

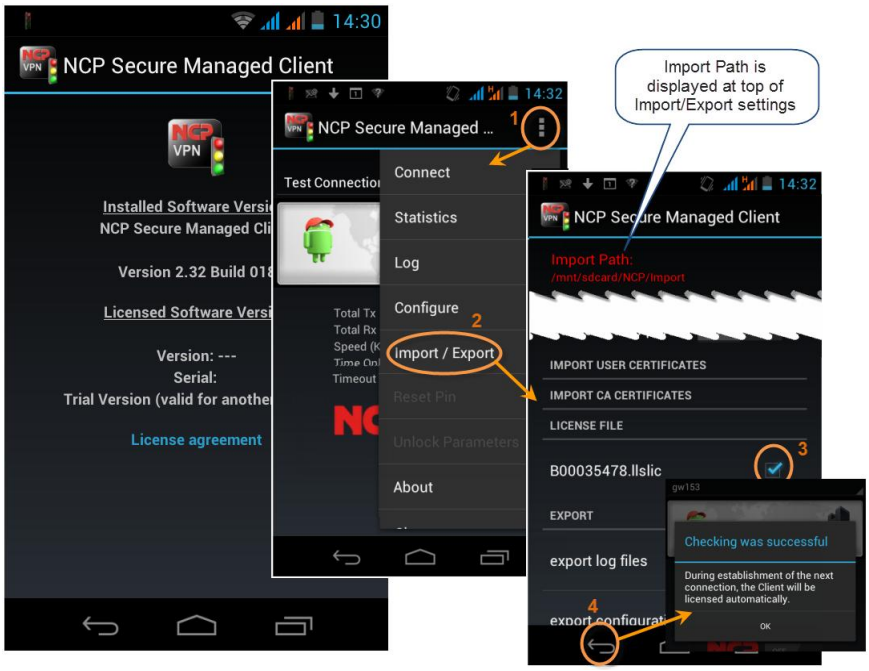
Licensing an individual NCP Secure Android Client Volume Edition is a two step process as follows:

1. <u>Import the Initialization File</u>

   Copy the Initialization File to the "Import Path".

   Import the file by opening the Import /Export settings and selecting the file under the "LICENSE FILE" header.

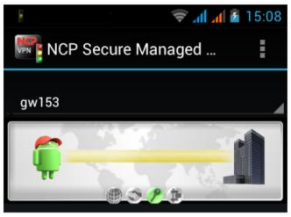
   NOTE: The "Checking was successful" message is only displayed if the import process completed successfully. Contact NCP support in the event that any other message is displayed at this point.



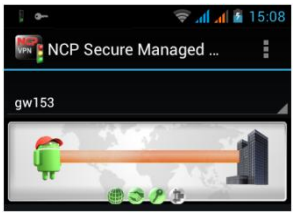
2. Complete the Client licensing by exchanging licensing details between Client and VLS via the Corporate VPN

   Establish a tunnel to the VPN gateway using the Connection Profile defined in step b) above. During the connection establishment the following takes place automatically

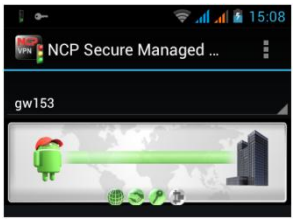
   i. the Client establishes a connection to the VPN gateway - the yellow, connection being established bar is displayed



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

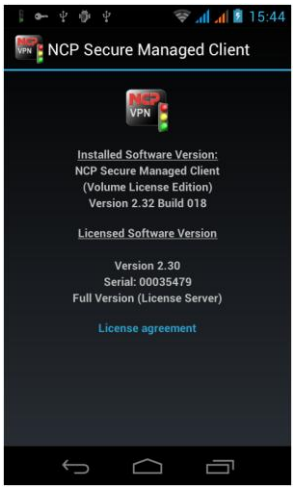


   iii. The next available license (serial number) will be selected and licensing details transmitted to the Client – the connection bar changes from orange to green.



   Licensing is now complete for this Client

   From this point onwards the Secure Android Client Volume Edition 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 Volume License Server – see section 4.4.



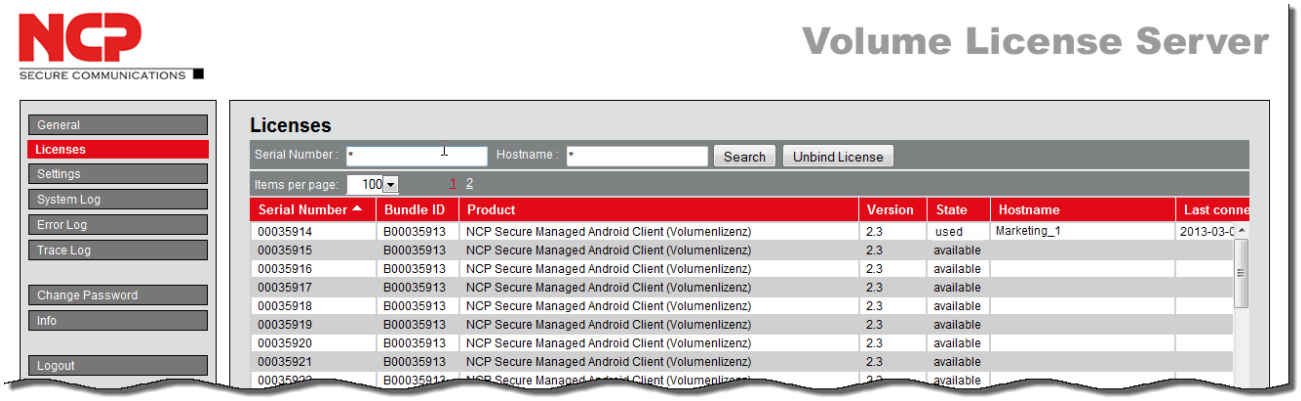
   NOTE: If an attempt is made to license a Client when all the licenses in a bundle have been used, then the message "Licensing operation failed" will be displayed and logged.

   NOTE: In steps ii. & iii. above, if a VPN connection is established and the onwards connection to the VLS 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 VLS cannot be established, the connection bar will remain orange. Check that the VLS is reachable from the VPN.

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

The "Licenses" display at the VLS console will look similar to the figure below:



The "State" column indicates the current state of each license/serial number:

"used"	If a Client has used a License, the Client's hostname is listed in "hostname" column. **NOTE:** (from VLS version 1.03 build 002 onwards) If the Client is an Android Client then the associated device's IMEI, if available, is displayed in the "hostname" column. If no IMEI is available then the device's hostname is displayed.
"available"	If the license is still available, i.e. has not been bound to a specific Client.

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 4.2 can be used to license any un-licensed Client.

4.4. Volume License Server Outages, and associated Client Recovery

Unless fundamental changes were made to the Volume 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 VLS 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.

NCP recommends that, in the case of a VLS 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 an NCP Secure Client – Juniper Edition 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.

4.5. Changing the VLS Machine's IP Address - and Licensing Implications

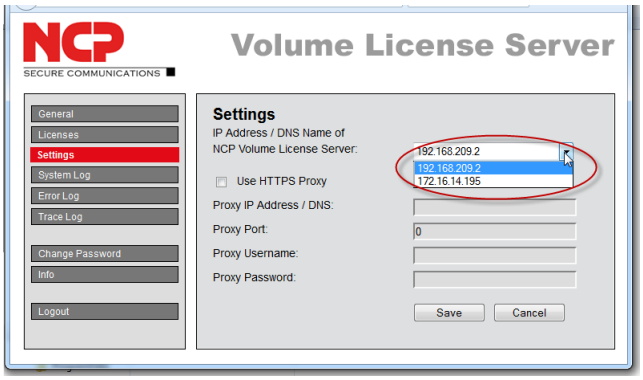
NCP strongly recommends that, when designing the network in which the VLS will be located, the VLS machine's IP address allocation be performed dynamically using DNS; this obviates the need for future changes such as described below.

If a change to the VLS 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.

4.5.1. Change the VLS machine's IP address

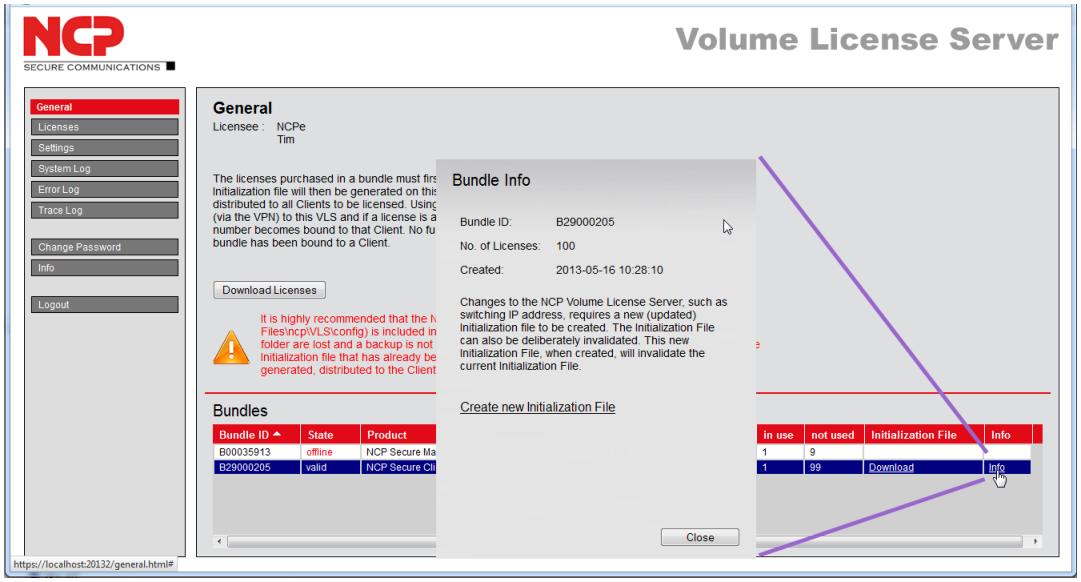
1. Change the machine's IP address using the appropriate functions in the underlying Windows operating system.
2. Open the "Settings" page and select the required IP address from the pulldown list. The list will display addresses for all adapters configured in the machine; it is important that the correct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



3. Enter Proxy details as necessary and press "Save".

4.5.2. 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"

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.

4.5.3. Relicense Affected Clients

As soon as the VLS machine's IP address is reconfigured (step 4.5.1 above), all attempts by Clients to connect to the VLS and validate their license will fail. Eventually attempts to establish a VPN tunnel will also fail and the Secure 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.

4.6. License Activation when Updating to a Newer Version of Secure Client software

When an NCP Secure Client must be updated to a newer version of the software and that version requires a new license - for example, from release 9.3x build yyy to release 9.40 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 Secure Client, 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 VLS configuration details - IP address, proxy IP address/port number - reflect the actual state of the VLS machine.

2) License the NCP Secure Client software - follow procedure in section 4.2. 3)

   After these two steps have been carried out, the license serial numbers from the original license bundle will no longer be available and attempts by NCP Secure Clients to validate their licenses will fail. The Secure Clients will be returned to the "Test License" / "Ready for Licensing" state, and when 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 step must be carried out without delay.

3) IMMEDIATELY establish a VPN tunnel to the VPN gateway.

When the VPN tunnel has been established, the Secure 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.

5. Clients - Versions supported by this VLS version

The following Secure Client versions are supported by this version of a VLS:

Secure Android Client Volume Edition: version 2.32 build 018 and later
Secure Client – Juniper Edition: version 9.25 build 005 and later

Note: at Juniper release 9.25 / 005, the VLS was referred to as a Local License Server (LLS) - when the product was subsequently renamed Volume License Server, functionality remained identical, both at Clients and the VLS.

6. Document Revision Status

Revision status is displayed on front page of document.

Revision	Changes
January 2012	First issue
May 2012	Client to VLS IP access port details included in Prerequisites
March 2013	Details added about of NCP Android Secure Managed Client / Secure Android Client Volume Edition.
June 2013	Added section 4.5 and details about port 12503 / SSL tunnel.
August 2013	Added section 4.6 IMEI / hostname for Android Client various text clarifications