NCP
SECURE COMMUNICATIONS

QuickStart Guide
high security remote access

The NCP Local License Server (LLS)

Using the LLS to Manage Secure Client – Juniper Edition Licenses

As of May 2012
version 1.00 build 014

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

Germany:
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)

Contents

1. Introduction

This manual describes:

- the concepts behind license management in connection with large numbers of NCP Secure Client – Juniper Edition (Clients)
- the functionality provided by NCP's Local License Server (LLS) in combination with those Clients, and
- the procedures that must be undertaken by Virtual Private Network (VPN) administration personnel to manage the Clients and their associated licenses.

2. Overview

The NCP Local License Server can be used to manage the distribution of licenses for the NCP Secure Client – Juniper Edition. Designed to simplify the management of Client licenses across a VPN infrastructure consisting of a large numbers of VPN Clients, the LLS maintains an inventory of licenses that have been purchased from NCP and manages the distribution of those licenses to the respective Clients. By making use of an organization's VPN infrastructure, the licensing transactions between Client and LLS are guaranteed to be secure against eavesdropping, tampering or theft.

2.1. NCP Client Product Licenses

Licenses to be managed via a Local 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 – Juniper Edition 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 Local 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 – Juniper Edition to one single Client machine for an unspecified period of time.
- The serial number is bound to a specific NCP Secure Client – Juniper Edition by running the Licensing Wizard (a part of the Client Activation Wizard) at the Client machine.
- 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 Client – Juniper Edition using the LLS

Licenses purchased for use with a Local License Server are distributed to each NCP Secure Client – Juniper Edition as follows:

- The local licensing application – the Local License Server - runs on a Microsoft Windows based server.

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

  NOTE: The Local License Server must be allocated a fixed IP Address within the IP address domain of the organization's VPN infrastructure. This can be assigned either statically at the server or dynamically via the organization's DNS service. If the LLS IP address is dynamically assigned, the same DNS service MUST be accessible by all Client machines.

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

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

- A bundle of licenses is entered into the LLS database via the web console.

- After validating the bundle details with the NCP Activation Server and transferring the appropriate license information from the NCP Activation Server, a single Initialization File is automatically generated at the LLS.

  NOTE: The IP address (or fully qualified domain name if DNS is in use) of the LLS is one of the items stored in this file. If, for any reason, the IP Address of the LLS changes in the future, all Clients licensed via this LLS (i.e. with the original IP Address) will no longer be able to communicate with the LLS 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 LLS IP Address is liable to change in the future, you are advised to do the following:

  1. assign a DNS name to the LLS
  2. allocate an IP Address to that DNS name in the organization's DNS service
  3. ensure that all VPN Clients can obtain the LLS IP Address by resolving it via a DNS lookup.

  See also section 4 - LLS Server Outages, Backups and Recovery

- The Initialization File must be downloaded to a portable media (CD/DVD, USB stick etc.) and is used to activate any NCP Secure Client – Juniper Edition that can connect to the organization's VPN gateway.

- At each Client machine the appropriate NCP Secure Client – Juniper Edition software package must be installed before carrying out the licensing process.

- Licensing of each Client using the LLS should be carried out during the standard 30 day test period (which starts when the Client software is first installed).

- The licensing process uses information in the Initialization File, in combination with information from the LLS, to bind a serial number to that Client and license that Client.

  NOTE: One of the two following procedures must be used for reading the Initialization File (the choice will be dependent on customer specific circumstances):

1. Call the Licensing Wizard from the Client Monitor menu - the Wizard prompts the user to browse to the location of the Initialization File and select it. The Client will then automatically establish a VPN connection, exchange licensing information with the LLS and, after this, the Client will then be fully licensed.
2. Before starting the Client Monitor, store the Initialization File in the Client's installation directory (see the Client User Manual for location of the Installation directory). The next time the Client Monitor is started, the Initialization File will be imported. The Client will then automatically establish a VPN connection and exchange licensing information with the LLS. At this point the Initialization File located in the installation directory will be deleted and after this the Client will then be fully licensed.

- On licensing the Client, the LLS database is updated with the following details:
  - NCP Secure Client – Juniper Edition 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 Wizard 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 Licensing Wizard at that Client.
- As the database of Client to serial number bindings is stored at the LLS, each Client must periodically check its status at the LLS, a check that can only 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 wizard), no other VPN traffic is allowed.

2.3. LLS 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 LLS.

2.3.1. Recommended Backup and Restore Procedure.

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

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

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

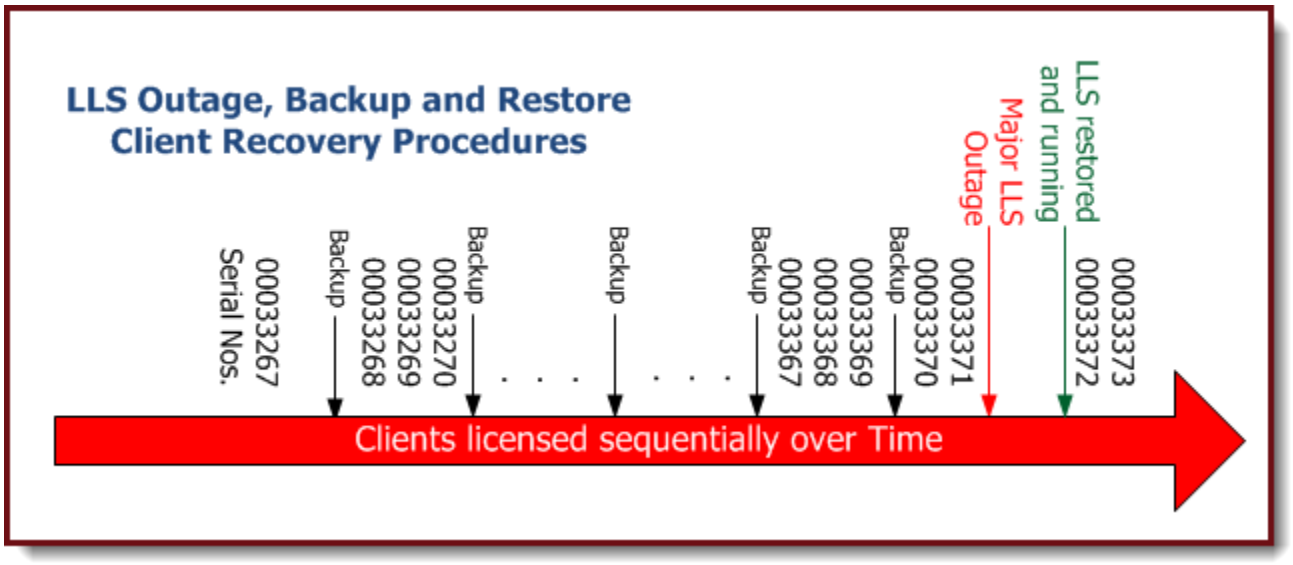
C:\Program Files\ncp\LLS\config

be performed on a regular basis.

If an LLS outage occurs which requires a recovery:

- Reinstall or recover the OS using standard procedures
- Reinstall the Local License Server software – see section 4
- Copy the latest backup of the configuration LLS folder to:
  default location C:\Program Files\ncp\LLS\config\

The diagram on the next page illustrates details of any Client recovery procedures that might be necessary.



After the LLS 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 LLS 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 LLS web interface Licenses display
  - user support procedures should signal the LLS 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).
- Clients that would receive serial numbers 00033372 and 00033373 can be licensed as normal.

3. Installing and Operating a Local License Server

3.1. Installation Prerequisites

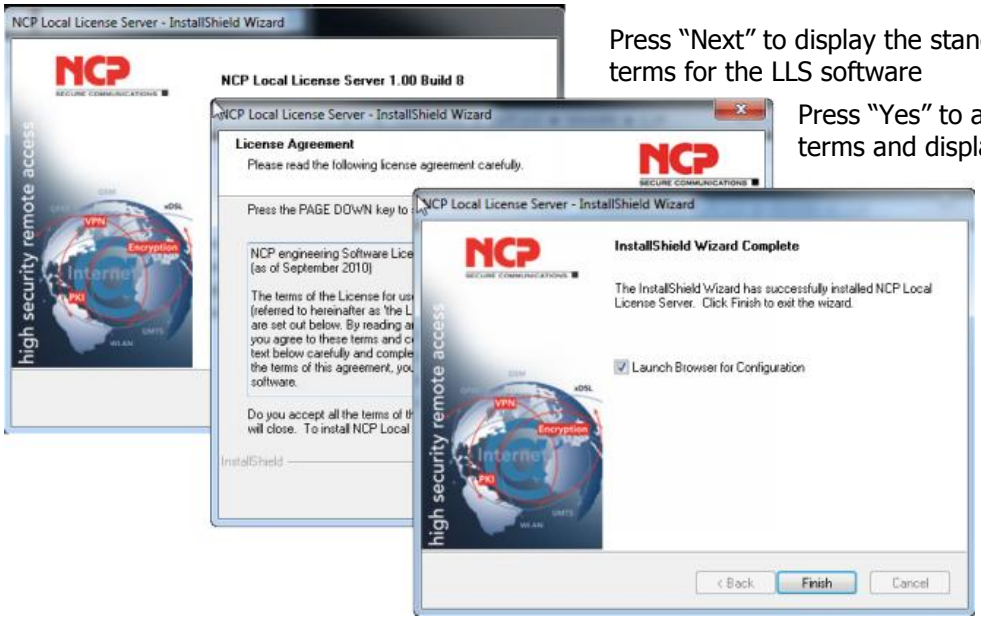
Server	Hardware: Any commercially available Intel X86 based machine. Backup Device: backup device with sufficient capacity to hold regular system backups – see section 2. Operating System: Microsoft Windows (32 or 64 bit): MS Windows XP or newer MS Windows Server 2003 or newer OS Services to be started or stopped: None specific to the LLS service
Network	VPN Subnet: The LLS must be accessible from the VPN subnet at all times. Client to LLS IP access (Firewall port): Port 12503/TCP on the LLS machine must be accessible from the Client. Internet: The LLS builds an SSL VPN connection to the NCP Activation Server. An HTTPS proxy IP address can be configured at the LLS 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 5 or later The web browser can optionally be hosted on the LLS server machine if this has the necessary graphics support. Browser to Server Authentication Certificates: During LLS installation a self-signed browser–server certificate is automatically generated. This is used to authenticate the web console browser with the LLS. Web Console to LLS IP access (Firewall port): Port 20132/TCP on the LLS machine must be accessible from the web console machine.
NCP Secure Clients	The following NCP Secure Clients can be licensed using the LLS: NCP Secure Client – Juniper Edition version 9.25 and later

3.2. Installation

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

a) Install Local License Server Software

- Download the LLS 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_LLS_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 LLS 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 LLS 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.

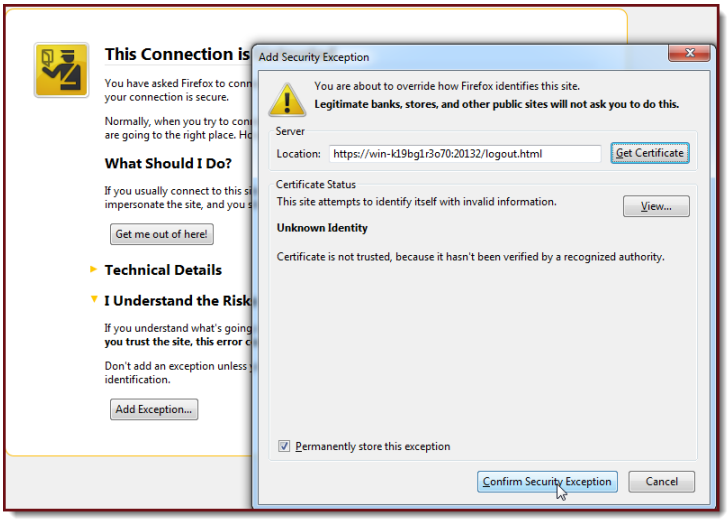
b) Call the LLS Administration Web Console

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

https://DNS_LLS:20132
where DNS_LLS is either the IP address or DNS name of the LLS

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 LLS server.

d) Define an LLS administrator password

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

Enter a suitable password and

press "Login"

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

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

3.3. Operating the LLS

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

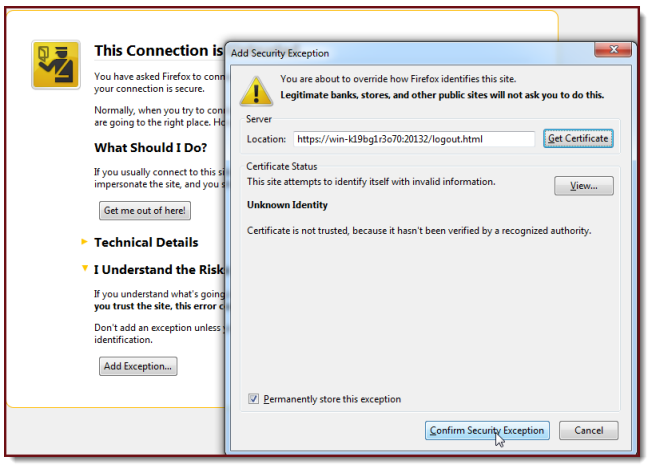
3.3.1. Starting and Stopping the LLS application/service

The LLS 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 LLS application/service.

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

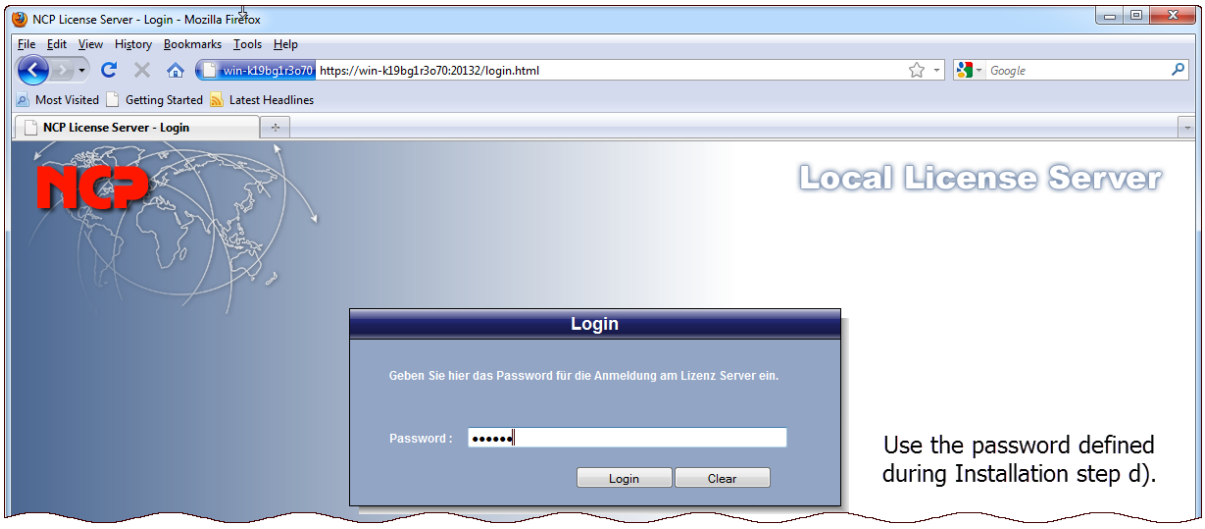


Get the certificate

and then

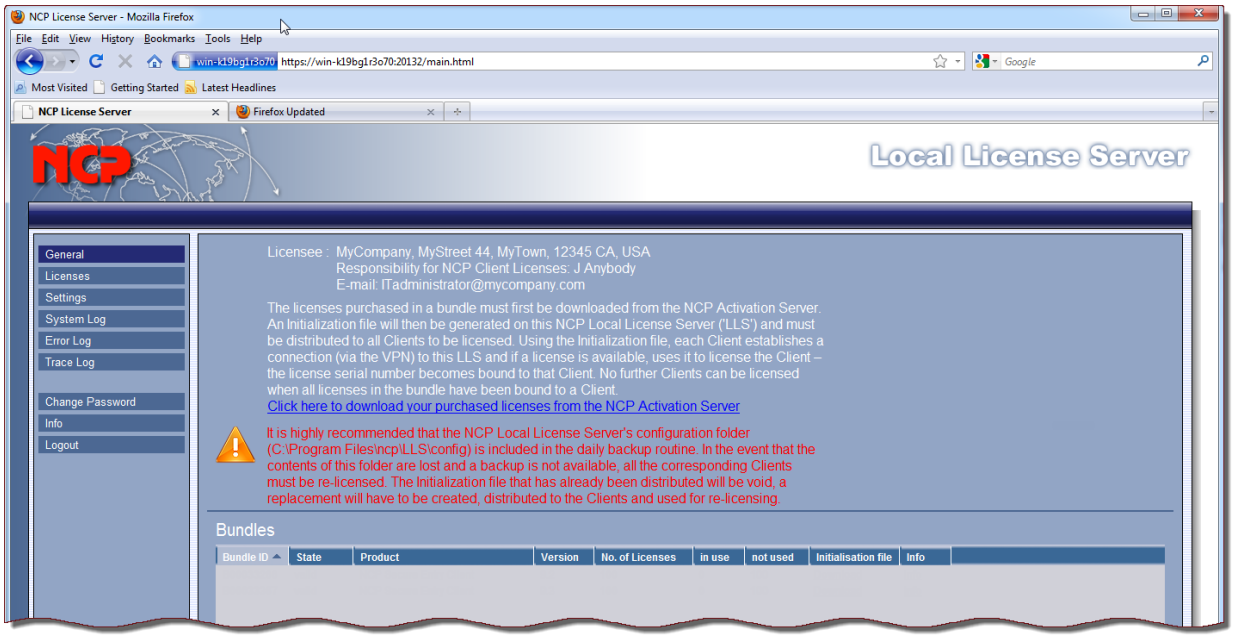
Confirm the security exceptions at the browser. (All subsequent connections between this the browser and LLS will use the certificate to mutually authenticate each other.).

The Login screen is then automatically displayed.



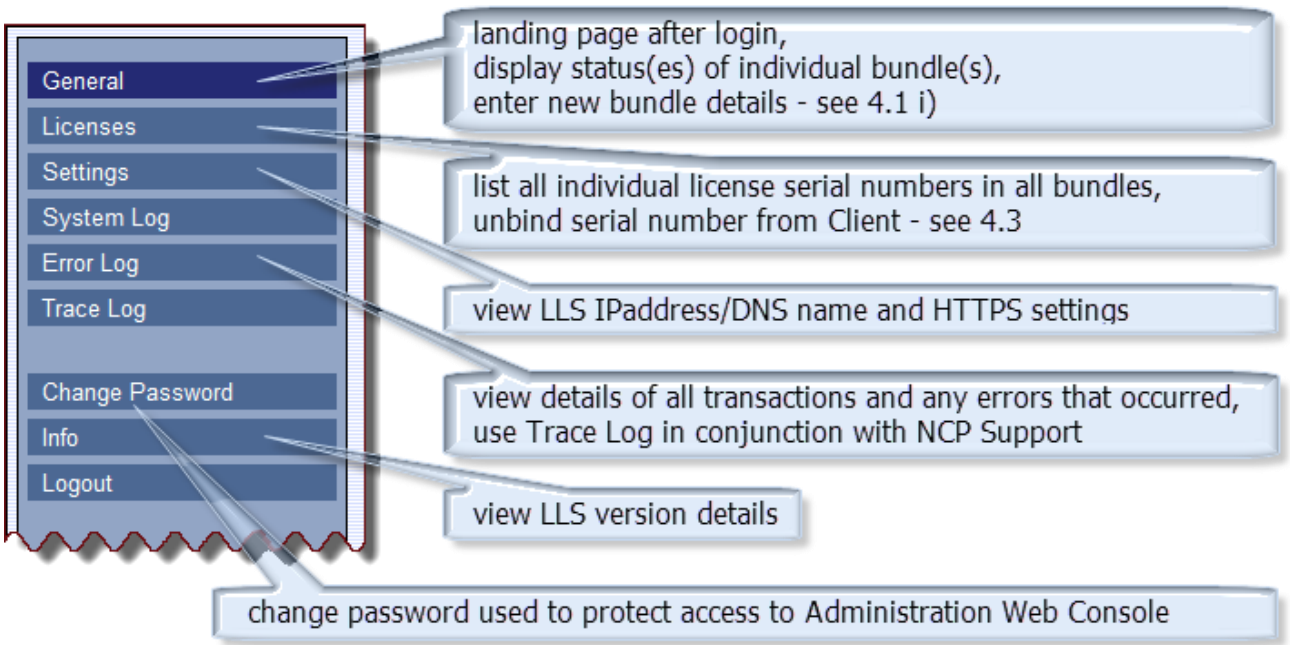
Use the password defined during Installation step d).

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



3.3.3. Overview of LLS Administration Web Console Menu

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



4. Managing Licenses

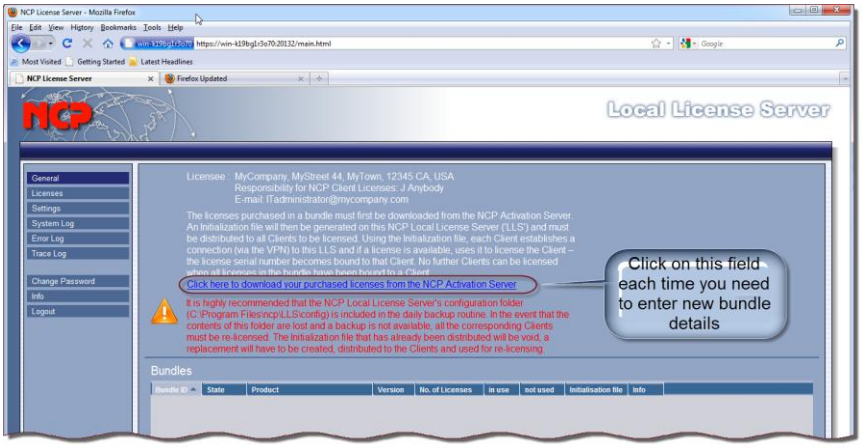
This section describes in detail how license bundles are downloaded to the Local License Server and how Client licensing is performed

4.1. Setting up the LLS after Installation

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

a) Login to the LLS Web Console

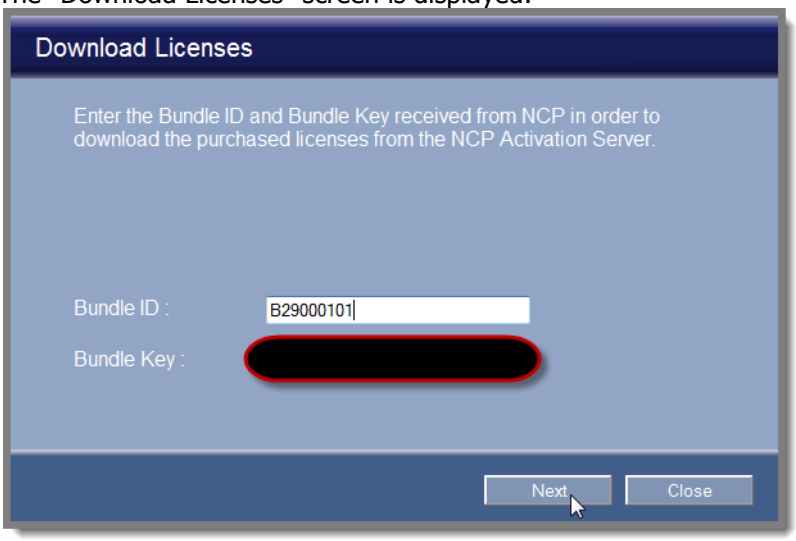
Login to the LLS web console using the browser, as described in section 3. The LLS General screen is displayed but without any Licensee details (as this is the first time the LLS has been accessed):



Click on the link as indicated.

b) Enter Bundle Details

The "Download Licenses" screen is displayed:



Enter the details provided by NCP in the respective fields

Press "Next" to continue

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

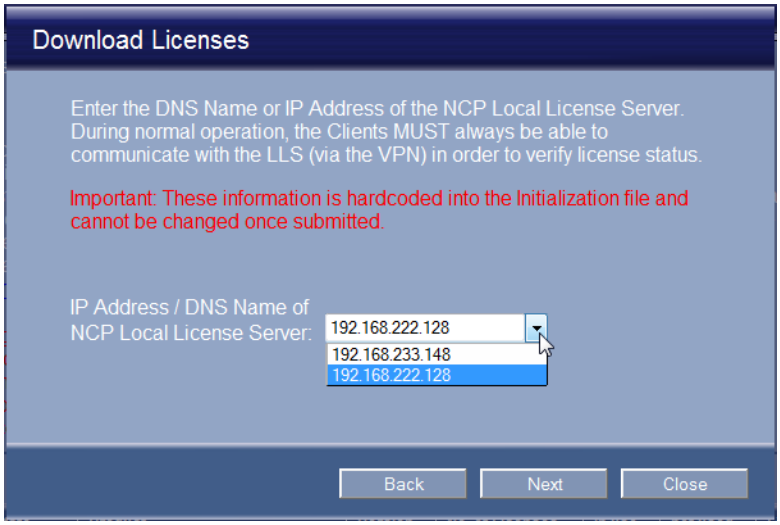
As this is the first bundle being entered into the LLS's database, you are now prompted to enter Licensee details. The 3 lines are free format and are displayed at each Client when it has been licensed.

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

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

d) Select IP Address or enter DNS Name

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



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

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

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

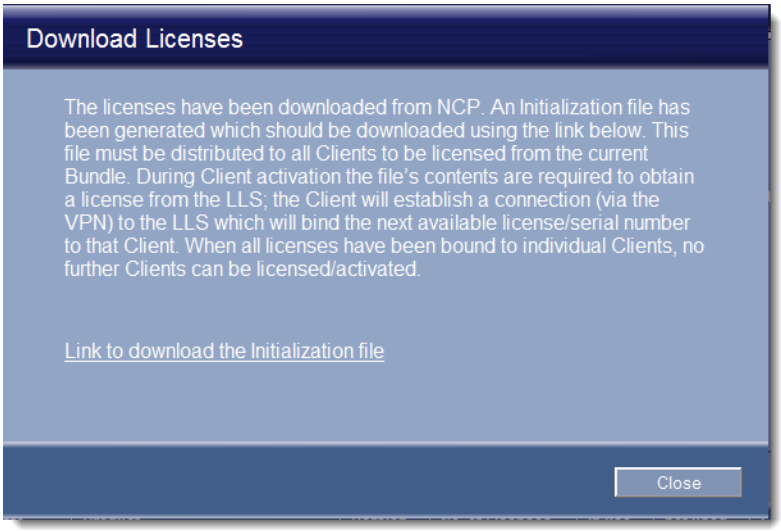
NOTE: Changing the LLS IP Address at any point after it is configured here will cause all currently licensed Clients to become unlicensed – they would be unable to undertake the regular validation of their licenses against the LLS database. You are advised to contact NCP support if it becomes necessary to change the LLS 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 LLS 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 LLS establishes a connection to the NCP Activation Server and the license details associated with the bundle selected are downloaded to the LLS. The Initialization File is then generated and can be downloaded to any media (USB stick etc.) accessible via the web console machine.

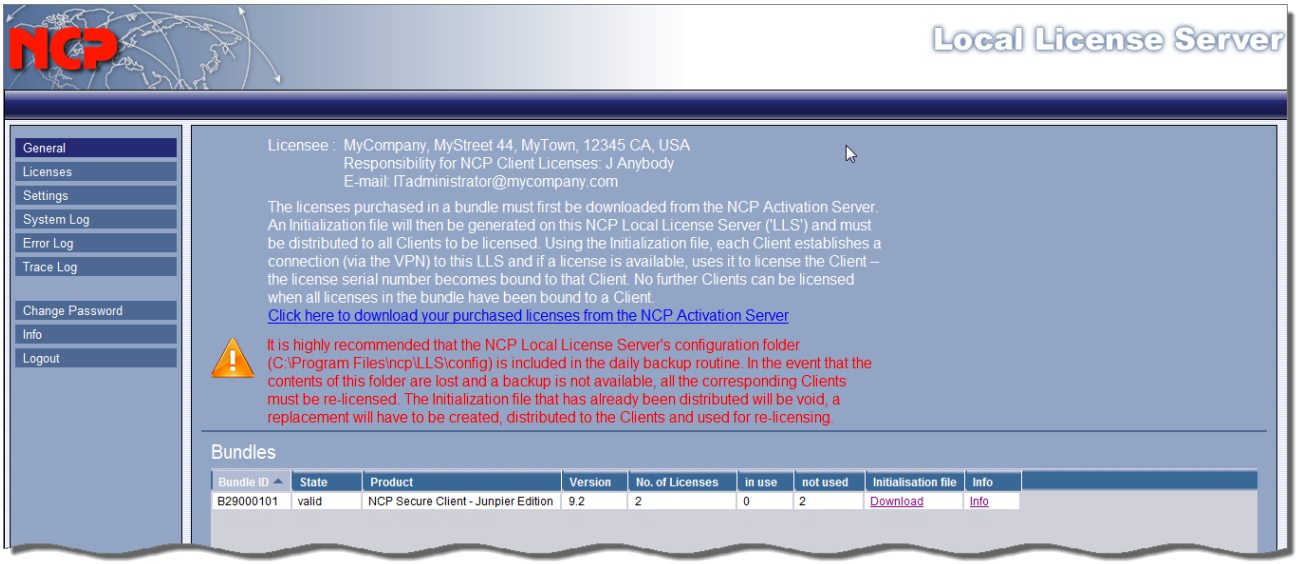


If you wish to download the Initialization File immediately, click the link here and download the file (see details in Section 4.1 j) and press "Close",

otherwise just press "Close"

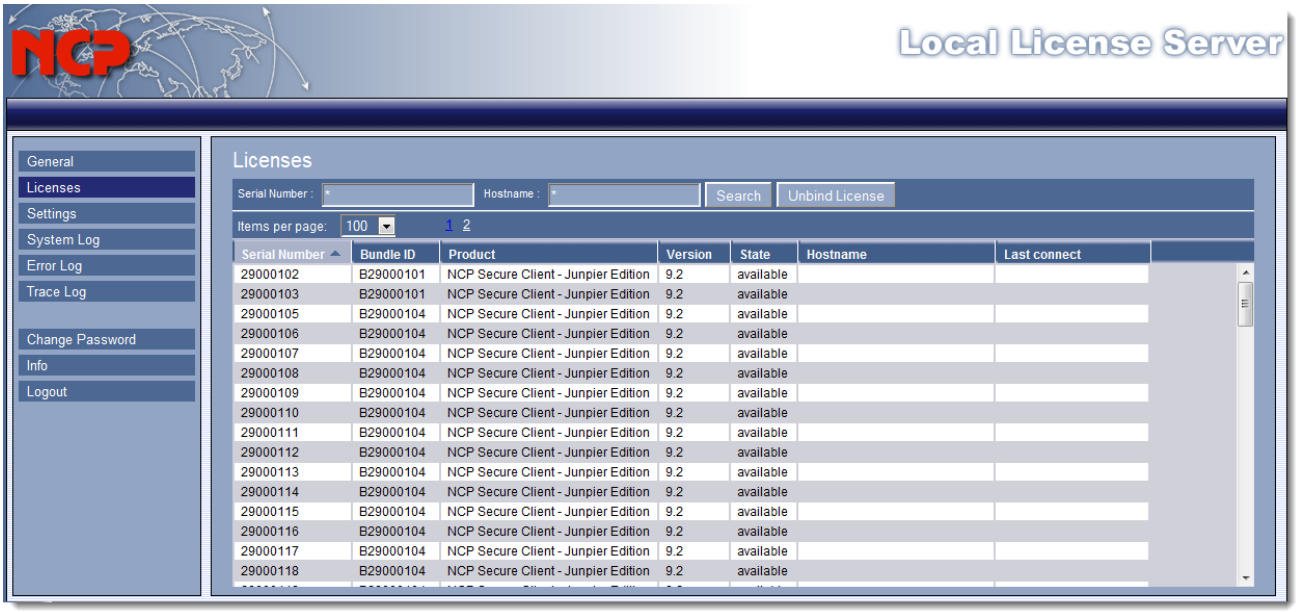
g) License Details now stored in LLS

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.



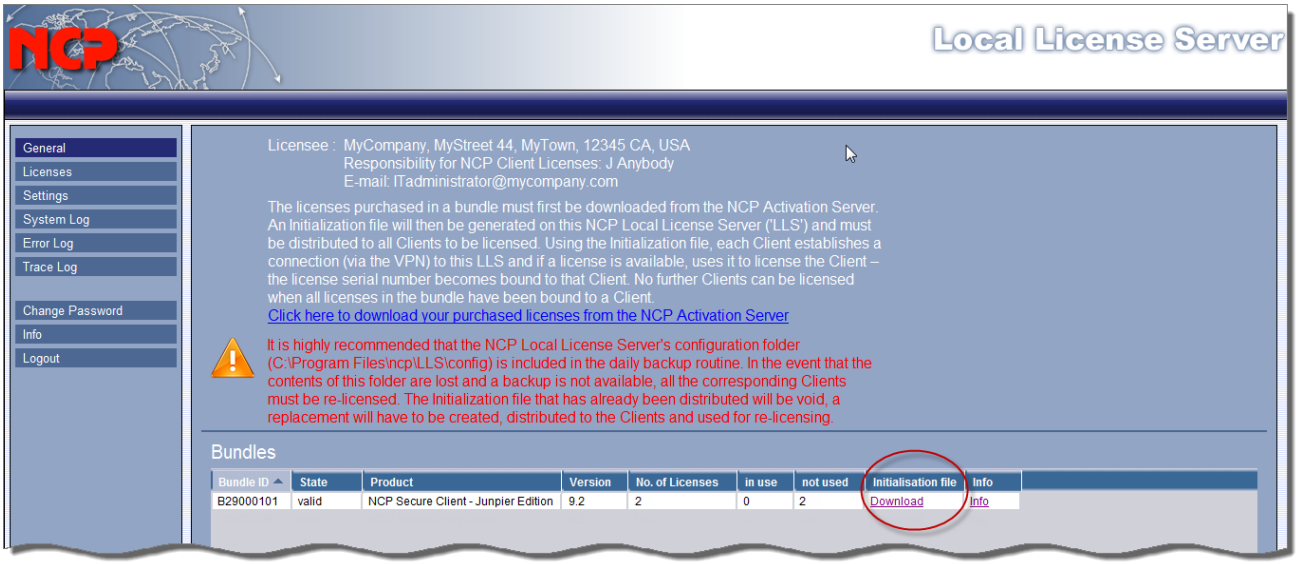
h) Displaying Bundle Details - Serial Numbers Used / Available etc.

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 LLS.

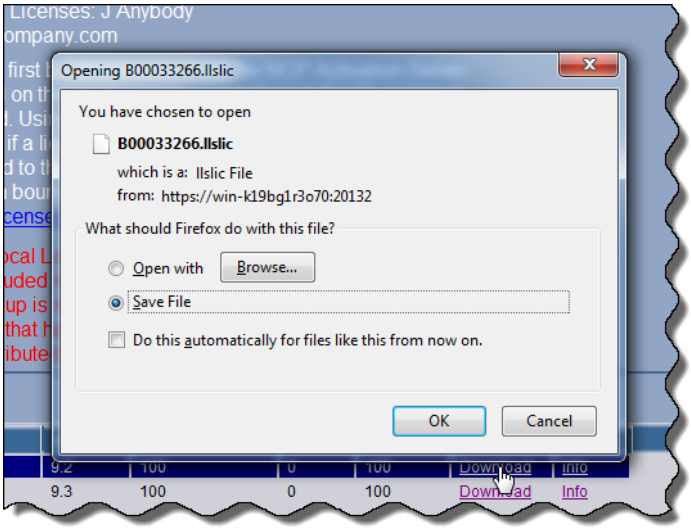


i) Downloading the Client Initialization File

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.

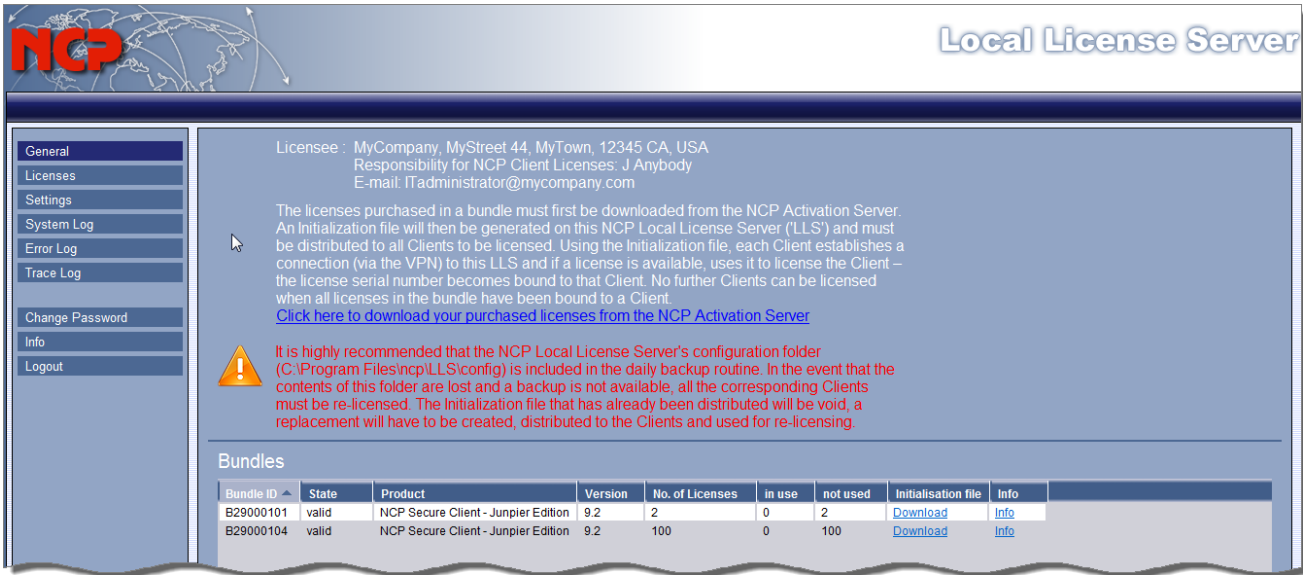


In the browser's download window select the "Save file" option and browse to the location where you wish to save the file. This is the file that will be used for Licensing the Clients – see Section 4.2

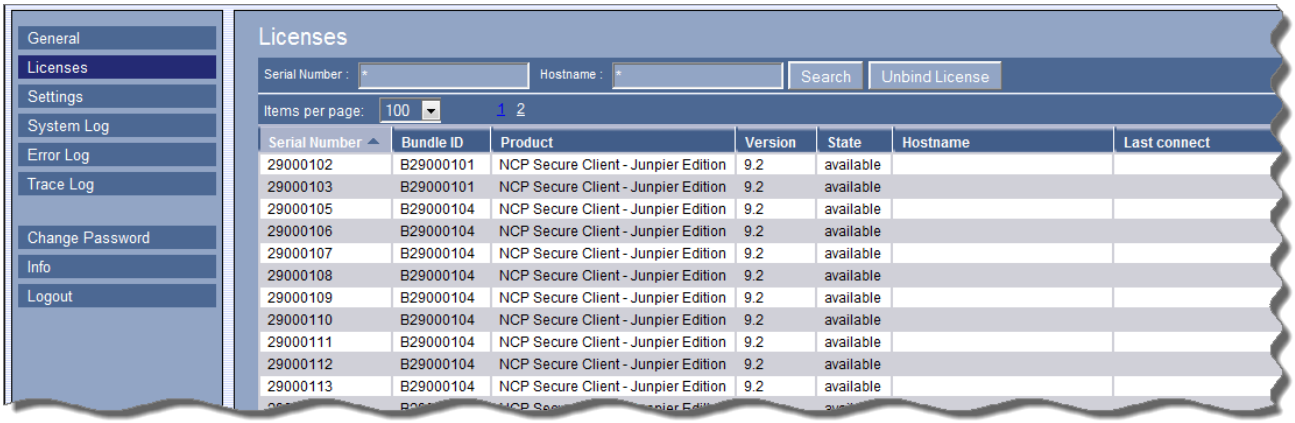
NOTE: This file can only be used to license Clients that correspond to the Product and Version Number defined in the original bundle.

j) Adding Additional Bundles

Use the procedures in steps b) and f) and g) to add additional bundles to the LLS'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 LLS are displayed in the "Licenses" screen. This list can be sorted by clicking on the header bar of the corresponding column to be sorted on.



4.2. Licensing Clients

The Initialization File created in step 4.1 i) must be distributed to all those Clients which are to be licensed. The exact distribution method is not described in this document as it is customer dependent.

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 Client Monitor - this will make use of the 30 day test license delivered with the Client.
- Create a default profile that enables a connection to be established to the corporate VPN gateway – this default profile will used by the Client's licensing process to communicate with the LLS.

c) License the Client Software

Licensing an individual Client is a two step process as follows:

1. Prepare the Client for Using a License Server

   As already discussed, there are two methods for importing the contents of the Initialization File:

   either

   - Call the Client Activation Wizard from the Client Monitor menu.
   - When prompted, browse to the location of the Initialization File and select that file.

   or

   - Store the Initialization File in the Client's installation directory and start the Client Monitor. **Note:** 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.

   On exiting from the Wizard, the activation status is displayed in the lower frame of the Client Monitor:

   A connection to the LLS is now required to complete the activation.

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

   The user must now establish a connection to the corporate VPN. During this connection establishment the following takes place automatically

   a) The Client establishes a connection to the VPN gateway

   b) The Client Licensing software establishes a connection to the Local License Server - the connection bar in the Client Monitor changes from yellow to orange.

   c) 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 Client is fully licensed and can establish VPN connections as freely required. No further activity is required in connection with licensing UNLESS there is an outage at the Local License Server – see section 4.4.

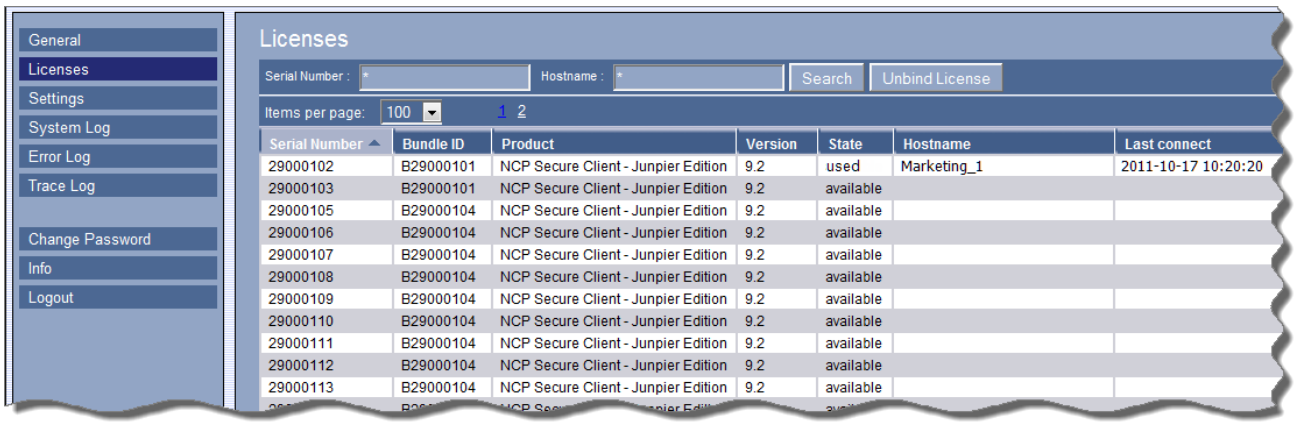
NOTE: If an attempt is made to license a Client when all the licenses in a bundle have been used, then the message "Licensing operation failed" will be displayed and logged.

NOTE: In steps b/c) above, if a VPN connection is established and the onwards connection to the LLS is established immediately , the connection bar will only flash orange briefly before switching to green.

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

4.3. Transferring Licenses between Clients – License Bind and Unbind

The "License" display at the LLS console will look similar to the diagram below:



Serial Number	Bundle ID	Product	Version	State	Hostname	Last connect
29000102	B29000101	NCP Secure Client - Junpier Edition	9.2	used	Marketing_1	2011-10-17 10:20:20
29000103	B29000101	NCP Secure Client - Junpier Edition	9.2	available		
29000105	B29000104	NCP Secure Client - Junpier Edition	9.2	available		
29000106	B29000104	NCP Secure Client - Junpier Edition	9.2	available		
29000107	B29000104	NCP Secure Client - Junpier Edition	9.2	available		
29000108	B29000104	NCP Secure Client - Junpier Edition	9.2	available		
29000109	B29000104	NCP Secure Client - Junpier Edition	9.2	available		
29000110	B29000104	NCP Secure Client - Junpier Edition	9.2	available		
29000111	B29000104	NCP Secure Client - Junpier Edition	9.2	available		
29000112	B29000104	NCP Secure Client - Junpier Edition	9.2	available		
29000113	B29000104	NCP Secure Client - Junpier Edition	9.2	available		

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

4.4. Local License Server Outages, and associated Client Recovery

Unless fundamental changes were made to the Local 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 an LLS 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 an LLS 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.

5. Document Revision Status

Revision status is displayed on front page of document.

Revision	Changes
January 2012	First issue
May 2012	Client to LLS IP access port details included in Prerequisites