



Hewlett Packard
Enterprise

HPE AutoPass License Server

Software Version: 9.2

Windows®, Linux and CentOS operating systems

User Guide

Document Release Date: April 2016

Software Release Date: April 2016

Legal Notices

Warranty

The only warranties for Hewlett-Packard Development Company, L.P. products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2015 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:
<https://softwaresupport.hp.com>

This site requires that you register for an HPE Passport and sign in. To register for an HPE Passport ID, go to: **<https://hpp12.passport.hpe.com/hppcf/createuser.do>**

Or click the **the Register** link at the top of the HPE Software Support page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Support

Visit the HPE Software Support Online web site at: <https://softwaresupport.hp.com>

This web site provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to:

<https://hpp12.passport.hp.com/hppcf/createuser.do>

To find more information about access levels, go to:

<https://softwaresupport.hp.com/web/softwaresupport/access-levels>

HPE Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this Web site is <http://h20230.www2.hp.com/sc/solutions/index.jsp>

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Chapter 1: Welcome to HPE AutoPass License Server	10
Chapter 2: Before You Install	11
Chapter 3: Installation and Setup	12
AutoPass License Server Setup and Start	12
SMTP Mail Configuration	13
SSL Configuration	13
Installing a Certificate from a Certificate Authority	17
Installation and Setup - Troubleshooting and Limitations	18
Chapter 4: AutoPass License Server Introduction	21
Chapter 5: AutoPass License Server Configuration	22
Concepts	23
AutoPass License Server Configuration - Overview	23
Reference	24
Main Configuration Tab (Configuration Pane)	24
SSL Configuration	26
SMTP Mail Configuration	30
Installing a Certificate from a Certificate Authority	30
AutoPass License Server Configuration - Frequently Asked Questions	31
Chapter 6: Integration with HP Usage Hub	34
Concepts	35
Usage Hub Configuration Overview	35
Reference	36
Usage Hub Server Tab (Configuration Pane)	36
Usage Hub Configuration - Frequently Asked Questions	38
Chapter 7: AutoPass License Server Redundancy Configuration	39
Concepts	40

- AutoPass License Server Redundancy - Overview 40
- AutoPass License Server Redundancy - Considerations and Limitations 40
- Tasks 42
 - How to Configure AutoPass License Server Redundancy 42
- Reference 44
 - Redundancy Tab (Configuration Pane) 44
- AutoPass License Server Redundancy - Frequently Asked Questions 46
- AutoPass License Server Redundancy - Troubleshooting and Limitations 47

- Chapter 8: AutoPass License Server User and User Group Management 48
 - Concepts 49
 - AutoPass License Server Users - Overview 49
 - AutoPass License Server User Groups - Overview 49
 - User Group Privilege Levels 49
 - AutoPass License Server User Group Privilege Matrix 50
 - User and User Group Sources 51
 - Tasks 53
 - How to Manage AutoPass License Server Users and User Groups 53
 - Reference 57
 - Users Tab (User Management Pane) 57
 - User Groups Tab (User Management Pane) 59
 - User Management Tab (Configuration Pane) 62
 - LDAP Tab (Configuration Pane) 65
 - AutoPass License Server User and User Group Management - Frequently Asked Questions 67
 - AutoPass License Server User and User Group Management - Troubleshooting and Limitations 69

- Chapter 9: License Management 70
 - Concepts 71
 - Installing Licenses 71
 - License Usage Reports 71
 - Searching License Check In and History 72
 - Archiving and Restoring Licenses 73
 - Borrowing Licenses 73
 - License Clean Up 74
 - Tasks 74
 - How to Manage Licenses 74
 - Reference 79
 - License Usage Pane 79
 - Feature Report Page (License Usage Pane) 80
 - Search Criteria Page (License Usage Pane) 86
 - Search Results Page (License Usage Pane) 87

Install License Tab (License Management Pane)	89
License Management Tab (License Management Pane)	90
Archive License Tab (License Management Pane)	91
Borrow License Tab (License Management Pane)	92
Borrow License Request Window (Borrow License Tab)	94
License Clean Up Tab (License Management Pane)	95
License Management - Frequently Asked Questions	96
License Management - Troubleshooting and Limitations	99
Chapter 10: Client User Management	101
Concepts	102
License Server Client Users - Overview	102
Client User Attributes	103
AutoPass License Server Client User Pools	104
License Usage by User Pools	104
License Reservation Priority	106
Feature-Based vs. Product Based Reservation	106
Restricting or Blocking User Pools	107
Tasks	109
How to Manage Client User Access	109
Reference	112
Pool Management Tab	112
Pool User List Section (Pool Management Tab)	113
Configuring Case Insensitivity	114
Pool to Product Mapping List (Pool Management Tab)	115
Featured-Based/Product-Based Reservation Tab	116
Client User Management - Frequently Asked Questions	119
Client Users Management - Troubleshooting and Limitations	121
Chapter 11: Remote Commuter License Management	122
Concepts	123
Commuter Licensing - Overview	123
Commuter License Check In and Check Out	123
Recovering Commuter Licenses	124
Tasks	125
How to Perform Remote Commuter License Operations	125
Reference	127
Check In/Check Out Tab (Remote Commuter Pane)	127
Remote Commuter Licensing Management - Frequently Asked Questions	129
Remote Commuter Licensing Management - Troubleshooting and Limitations	130

Chapter 1: Welcome to HPE AutoPass License Server

Welcome to HPE AutoPass License Server, the HPE Web-based solution for managing your HPE software product licenses. AutoPass License Server helps you organize and manage your product licenses, server users, and client users.

This guide describes how to install, set up, and use the HPE AutoPass License Server.

This guide is intended for users who will install and administer the AutoPass License Server. Users should have some knowledge of system administration.

Chapter 2: Before You Install

The HPEAutoPass License Server User Guide provides the information you need to install and use the HPEAutoPass License Server.

To successfully install and run the HPE AutoPass License Server, your computer must meet the minimum system requirements shown below. However, performance may be improved by using systems with stronger/later setups than the minimum requirements.

For a list of all supported operating systems, see the *HPE AutoPass License Server Product Availability Matrix*, available from the root folder of the DVD. The most up-to-date product availability matrix is available from the HPE Software Product manuals site, at <http://h20230.www2.hp.com/selfsolve/manuals> (requires an HPE passport).

Computer Processor	1.6 Ghz or higher
Operating System	Windows 2008 SP1 64 bits Red Hat Enterprise Linux 7 x64-bits CentOS 7.0
Memory	A minimum of 1 GB of RAM
Color Settings	High Color (16-bit)
Graphics Card	Graphics card with 64 MB video memory
Protocols	HTTPS must be enabled for products and users who use the AutoPass License Server.
Port	Port 5814 must be accessible for products and client users to connect to the AutoPass License Server. Note: This is the port number registered with the Internet Assigned Number Authority (IANA) for HPE products.
Web Browser	<ul style="list-style-type: none">• Mozilla Firefox 39• Internet Explorer 11• Google Chrome 40

Chapter 3: Installation and Setup

Before you begin using the AutoPass License Server, you must install and set up the AutoPass License Server.

Before installing, make sure your AutoPass License Server host computer meets the minimum system requirements. For details, see ["Before You Install" on page 11](#).

If you are migrating from 8.3.X to 9.1, refer to the [HPE AutoPass License Server_Migration](#) document.

This chapter includes the following sections:

- ["Installation" on page 1](#)
- ["Uninstallation" on page 1](#)
- ["AutoPass License Server Setup and Start" below](#)
- ["Installation and Setup - Troubleshooting and Limitations" on page 18](#)

AutoPass License Server Setup and Start

After installation, the AutoPass License Server is automatically started as a Windows service. The license for the AutoPass License Server is provided with the installation. No additional special setup is required

To launch the AutoPass License Server, enter the server's Web address into your browser: `https://<ip address or Host Name>:5814/autopass`.

Use the following credentials for the initial login to the AutoPass License Server:

- **User name:** *admin*
- **Password:** *password*

After the initial login, you are required to change the password. You can also create other AutoPass License Server users with login credentials and access permissions after the initial login. For details, see ["AutoPass License Server User and User Group Management" on page 48](#).

You are also required to configure the mail server after the initial login. In addition, you can configure other general AutoPass License Server settings, including:

- Server configuration settings
- License checkout history purge settings
- Audit reporting settings
- Expiration notice settings
- License borrowing settings
- Server redundancy settings.

For details, see ["AutoPass License Server Configuration" on page 22](#) and ["AutoPass License Server Redundancy Configuration" on page 39](#).

SMTP Mail Configuration

Simple Mail Transfer Protocol (SMTP) communications servers use transport-layer security (TLS) or SSL encryption which provides privacy and authentication. The mail configuration secures the SMTP sessions using the STARTTLS property mentioned below in **mailconfig.properties** file in the path

\\HP\HP AutoPass License Server\AutoPass\LicenseServer\data\conf\.

“mail.smtp.starttls.enable” = true

Note: Configuring SMTP is mandatory if the password has to be reset.

SSL Configuration

To install and configure SSL support on Tomcat, you need to follow the below steps.

1. Create a keystore file to store the server's private key and self-signed certificate by executing the following command:

Windows:

```
"%JAVA_HOME%\bin\keytool" -genkey -alias tomcat -keyalg RSA
```

Unix:

```
$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA and specify a password value of "changeit".
```

2. Uncomment the "SSL HTTP/1.1 Connector" entry in \$CATALINA_BASE/conf/server.xml and modify as described in the section below.

Prepare the Certificate Keystore

Tomcat currently operates only on JKS, PKCS11 or PKCS12 format keystores. The JKS format is Java's standard "Java KeyStore" format, and is the format created by the keytool command-line utility. This tool is included in the JDK. The PKCS12 format is an internet standard, and can be manipulated via (among other things) OpenSSL and Microsoft's Key-Manager.

Each entry in a keystore is identified by an alias string. Whilst many keystore implementations treat aliases in a case insensitive manner, case sensitive implementations are available. The PKCS11 specification, for example, requires that aliases are case sensitive. To avoid issues related to the case sensitivity of aliases, it is not recommended to use aliases that differ only in case.

To import an existing certificate into a JKS keystore, please read the documentation (in your JDK documentation package) about keytool. Note that OpenSSL often adds readable comments before the key, but keytool does not support that. So if your certificate has comments before the key data, remove them before importing the certificate with keytool.

To import an existing certificate signed by your own CA into a PKCS12 keystore using OpenSSL you would execute a command like:

```
openssl pkcs12 -export -in mycert.crt -inkey mykey.key
```

-out mycert.p12 -name tomcat -CAfile myCA.crt
-caname root -chain

For more advanced cases, consult the OpenSSL documentation.

To create a new JKS keystore from scratch, containing a single self-signed Certificate, execute the following from a terminal command line:

Windows:

```
"%JAVA_HOME%\bin\keytool" -genkey -alias tomcat -keyalg RSA
```

Unix:

```
$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA
```

(The RSA algorithm should be preferred as a secure algorithm, and this also ensures general compatibility with other servers and components.)

This command will create a new file, in the home directory of the user under which you run it, named ".keystore". To specify a different location or filename, add the `-keystore` parameter, followed by the complete pathname to your keystore file, to the keytool command shown above. You will also need to reflect this new location in the `server.xml` configuration file, as described later. For example:

Windows:

```
"%JAVA_HOME%\bin\keytool" -genkey -alias tomcat -keyalg RSA  
-keystore \path\to\my\keystore
```

Unix:

```
$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA  
-keystore /path/to/my/keystore
```

After executing this command, you will first be prompted for the keystore password. The default password used by Tomcat is "changeit" (all lower case), although you can specify a custom password if you like. You will also need to specify the custom password in the `server.xml` configuration file, as described later.

Next, you will be prompted for general information about this Certificate, such as company, contact name, and so on. This information will be displayed to users who attempt to access a secure page in your application, so make sure that the information provided here matches what they will expect.

Finally, you will be prompted for the key password, which is the password specifically for this Certificate (as opposed to any other Certificates stored in the same keystore file). You **MUST** use the same password here as was used for the keystore password itself. This is a restriction of the Tomcat implementation. (Currently, the keytool prompt will tell you that pressing the ENTER key does this for you automatically.)

If everything was successful, you now have a keystore file with a Certificate that can be used by your server.

Note: Your private key password and keystore password should be the same. If they differ, you will get an error along the lines of `java.io`.

Edit the Tomcat Configuration File

Tomcat can use two different implementations of SSL:

- The JSSE implementation provided as part of the Java runtime (since 1.4)
- The APR implementation, which uses the OpenSSL engine by default.

The exact configuration details depend on which implementation is being used. If you configured Connector by specifying generic protocol="HTTP/1.1" then the implementation used by Tomcat is chosen automatically. If the installation uses APR - i.e. you have installed the Tomcat native library - then it will use the APR SSL implementation, otherwise it will use the Java JSSE implementation.

As configuration attributes for SSL support significantly differ between APR vs. JSSE implementations, it is recommended to avoid auto-selection of implementation. It is done by specifying a classname in the protocol attribute of the Connector.

To define a Java (JSSE) connector, regardless of whether the APR library is loaded or not, use one of the following:

```
<!-- Define a HTTP/1.1 Connector on port 8443, JSSE BIO implementation -->  
<Connector protocol="org.apache.coyote.http11.Http11Protocol"  
port="8443" .../>  
<!-- Define a HTTP/1.1 Connector on port 8443, JSSE NIO implementation -->  
<Connector protocol="org.apache.coyote.http11.Http11NioProtocol"  
port="8443" .../>
```

Alternatively, to specify an APR connector (the APR library must be available) use:

```
<!-- Define a HTTP/1.1 Connector on port 8443, APR implementation -->  
<Connector protocol="org.apache.coyote.http11.Http11AprProtocol"  
port="8443" .../>
```

If you are using APR, you have the option of configuring an alternative engine to OpenSSL.

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"  
SSLEngine="someengine" SSLRandomSeed="somedevice" />
```

The default value is

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"  
SSLEngine="on" SSLRandomSeed="builtin" />
```

So to use SSL under APR, make sure the SSLEngine attribute is set to something other than off. The default value is on and if you specify another value, it has to be a valid engine name.

SSLRandomSeed allows to specify a source of entropy. Productive system needs a reliable source of entropy but entropy may need a lot of time to be collected therefore test systems could use no blocking entropy sources like "/dev/urandom" that will allow quicker starts of Tomcat.

The final step is to configure the Connector in the `$CATALINA_BASE/conf/server.xml` file, where `$CATALINA_BASE` represents the base directory for the Tomcat 6 instance. An example `<Connector>` element for an SSL connector is included in the default `server.xml` file installed with Tomcat. For JSSE, it should look something like this:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->  
<Connector  
protocol="org.apache.coyote.http11.Http11Protocol"  
port="8443" maxThreads="200"  
scheme="https" secure="true" SSLEnabled="true"  
keystoreFile="{user.home}/.keystore" keystorePass="changeit"  
clientAuth="false" sslProtocol="TLS"/>
```

The APR connector uses different attributes for many SSL settings, particularly keys and certificates. An example of an APR configuration is:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->  
<Connector  
protocol="org.apache.coyote.http11.Http11AprProtocol"  
port="8443" maxThreads="200"  
scheme="https" secure="true" SSLEnabled="true"  
SSLCertificateFile="/usr/local/ssl/server.crt"  
SSLCertificateKeyFile="/usr/local/ssl/server.pem"  
SSLVerifyClient="optional" SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"/>
```

The configuration options and information on which attributes are mandatory for the JSSE based connectors (BIO and NIO) are documented in the SSL Support section of the HTTP connector configuration reference. The configuration options and information on which attributes are mandatory for the APR connector are documented in the HTTPS section of the APR How-To.

The port attribute is the TCP/IP port number on which Tomcat will listen for secure connections. You can change this to any port number you wish (such as to the default port for https communications, which is 443). However, special setup (outside the scope of this document) is necessary to run Tomcat on port numbers lower than 1024 on many operating systems.

If you change the port number here, you should also change the value specified for the `redirectPort` attribute on the non-SSL connector. This allows Tomcat to automatically redirect users who attempt to access a page with a security constraint specifying that SSL is required, as required by the Servlet Specification.

After completing these configuration changes, you must restart Tomcat as you normally do, and you should be in business. You should be able to access any web application supported by Tomcat via SSL. For example, try:

`https://localhost:8443/`

and you should see the usual Tomcat splash page (unless you have modified the ROOT web application).

Installing a Certificate from a Certificate Authority

To obtain and install a Certificate from a Certificate Authority (like verisign.com, thawte.com or trustcenter.de), read the previous section and then follow these instructions:

Create a local Certificate Signing Request (CSR)

In order to obtain a Certificate from the Certificate Authority of your choice you have to create a so called Certificate Signing Request (CSR). That CSR will be used by the Certificate Authority to create a Certificate that will identify your website as "secure". To create a CSR follow these steps:

Create a local self-signed Certificate (as described in the previous section):

```
keytool -genkey -alias tomcat -keyalg RSA
```

```
-keystore <your_keystore_filename>
```

Note: In some cases you will have to enter the domain of your website (i.e. www.myside.org) in the field "first- and lastname" in order to create a working Certificate.

The CSR is then created with:

```
keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr
```

```
-keystore <your_keystore_filename>
```

Now you have a file called certreq.csr that you can submit to the Certificate Authority (look at the documentation of the Certificate Authority website on how to do this). In return you get a Certificate.

Importing the Certificate

Now that you have your Certificate you can import it into you local keystore. First of all you have to import a so called Chain Certificate or Root Certificate into your keystore. After that you can proceed with importing your Certificate.

- Download a Chain Certificate from the Certificate Authority you obtained the Certificate from.

For Verisign.com commercial certificates go to:

<http://www.verisign.com/support/install/intermediate.html>

For Verisign.com trial certificates go to: http://www.verisign.com/support/verisign-intermediate-ca/Trial_Secure_Server_Root/index.html

For Trustcenter.de go to: <http://www.trustcenter.de/certservices/cacerts/en/en.htm#server>

For Thawte.com go to: <http://www.thawte.com/certs/trustmap.html>

- Import the Chain Certificate into your keystore

```
keytool -import -alias root -keystore <your_keystore_filename>
```

```
-trustcacerts -file <filename_of_the_chain_certificate>
```

- And finally import your new Certificate

```
keytool -import -alias tomcat -keystore <your_keystore_filename>
```

```
-file <your_certificate_filename>
```

Installation and Setup - Troubleshooting and Limitations

What do I do if the AutoPass License Server failed to install?

If the automatic installation failed, you must manually install the AutoPass License Server.



To manually install the AutoPass License Server, do the following:

1. In the Command Prompt window, enter the directory path to the `<License Server installation>/bin` folder, as seen in the example below:

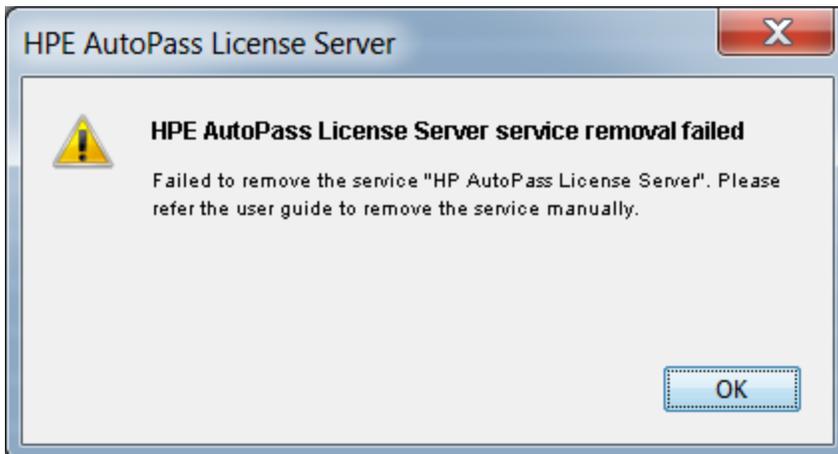
```
<installation directory>/HP Autopass License Server/HP Autopass License Server/bin>
```

2. After the `bin` directory path, enter the command `hpLicServer.bat install` and press **Enter**.

The AutoPass License Server is installed on the computer.

What do I do if the AutoPass License Server failed to uninstall?

If the automatic uninstallation failed, you must manually uninstall the AutoPass License Server.



To manually uninstall the AutoPass License Server, do the following:

1. In the Command Prompt window, enter the directory path to the <License Server installation>/bin folder, as seen in the example below:

```
<installation directory>\HP Autopass License Server\HP Autopass License Server\bin>
```

2. After the bin directory path, enter the command `hpLicService.bat remove` and press **Enter**.

The AutoPass License Server is then uninstalled from the computer.

What do I do if the AutoPass License Server failed to start?

If the automatic start of the AutoPass License Server following installation failed, you must manually start the AutoPass License Server.



To manually start the AutoPass License Server, do the following:

1. In the Command Prompt window, enter `services.msc`. The Windows Services dialog box opens.
2. In the Services (Local) list, right-click **HPE Autopass License Server**, and select **Start**.

The AutoPass License Server service is started and you can access the AutoPass License Server via the Web browser.

Chapter 4: AutoPass License Server

Introduction

The AutoPass License Server enables you to manage the concurrent licenses for your HPE software products.

Software product licenses are broadly classified into two types: **concurrent** (floating) and **seat** (standalone) licenses. A concurrent license is shared dynamically between multiple client users, whereas a seat license is locked to a specific client machine. The concurrent licenses are then shared or "pooled" between a group of users. Using concurrent licenses enables you to purchase the number of licenses equal to the largest number of users liable to be active at any time, instead of the total number of users of a product.

The AutoPass License Server manages the licenses acquired from the HPE license portal. These licenses are then installed on the AutoPass License Server.

When a client computer needs a license, the client sends a request to the AutoPass License Server and a license is checked out to this user. After the client user's work session (or when the license expires), the license is returned to the AutoPass License Server for renewal or for use by other users. If a client user does not have a regular connection to the AutoPass License Server, the client user can check out a commuter license from the AutoPass License Server.

Using the AutoPass License Server, you can:

- Control and managing how the licenses are used
- Create and manage users who are responsible for administering the AutoPass License Server and the licenses installed on the server
- Manage client user access to the AutoPass License Server.

Chapter 5: AutoPass License Server Configuration

This chapter includes:

Concepts

- ["AutoPass License Server Configuration - Overview" on the next page](#)

Reference

- ["Main Configuration Tab \(Configuration Pane\)" on page 24](#)
- ["AutoPass License Server Configuration - Frequently Asked Questions" on page 31](#)

Concepts

AutoPass License Server Configuration - Overview

After installing the AutoPass License Server, you should set configuration options for the AutoPass License Server.

Note: Configuration of mail settings is required upon the administrator's first login to the AutoPass License Server.

You set the configurations for a number of different options:

- Server Mail Configuration
- Check In History Purging
- Server Audit Reports
- AutoPass License Server Borrowing
- Expiration Notifications
- Server IP Configuration
- Server Discovery

For details about the individual options, see ["Main Configuration Tab \(Configuration Pane\)" on the next page](#)

Note: When logging into the AutoPass License Server for the first time, you must configure the mail settings for the server.

Reference

Main Configuration Tab (Configuration Pane)

The Main configuration tab enables you to configure general AutoPass License Server settings.

To access	Configuration pane > Main tab
Important information	You must configure the mail configuration settings after logging into the AutoPass License Server for the first time.

User interface elements are described below:

UI Element	Description
Mail Configuration	<p>Enables you to configure the settings for mail sent by the License Server.</p> <p>You can enter the following details:</p> <ul style="list-style-type: none">• Mail Server: The name of the server from which mail messages are sent from the AutoPass License Server. <i>(required field)</i>• Port: The port number from which mail messages are sent from the AutoPass License Server.• Admin Email: The sever administrator's email address to send server-related communications. <i>(required field)</i>• User Name: The server administrator user name. This user name is in addition to the user names created in the "Users Tab (User Management Pane)" on page 57. Default: <i>admin</i>• Password: The server administrator's user password.• Test Mail: A mail address to use for a test of the mail configuration settings. Click Send Mail after entering a mail address to test. <p>Refer "SMTP Mail Configuration" on page 30 for more details on SMTP Configuration.</p>
Concurrent License Purge Settings	<p>Enables you to set preferences for how often to delete the server operations history.</p> <ul style="list-style-type: none">• Auto Purge: Automatically clears the server operations history according to the settings indicated. Note: To stop automatic purging of the records, clear the check box.• Purge Records Older Than <> Days: Purges all records older than the number of days entered.• Maximum Records to Retain: The number of server operations to keep in the AutoPass License Server database, beginning with the most recent operations.

UI Element	Description
	<p>Note: You can also purge the history of server operations in the Search Results window. For details, see "Search Results Page (License Usage Pane)" on page 87.</p>
<p>Usage Hub Server Settings</p>	<p>Enables you view to the configuration settings of Usage Hub Server. Once settings are saved, the Usage Hub Server configuration tab is enabled. For more details refer "Usage Hub Server Tab (Configuration Pane)" on page 36</p> <p>Note: It is required to restart service for the changes to take effect.</p>
<p>Audit Configuration</p>	<p>Enables you set the preference for what is reported in the AutoPass License Server log for checkout and checkin requests and responses.</p> <p>You can choose to report one of the following levels:</p> <ul style="list-style-type: none"> • No Audit: No record of checkout or checkin requests (<i>default</i>) • Request: A record of all checkout and checkin requests. • Response: A record of all AutoPass License Server responses to license checkout and checkin requests. • Request and Response: A record of all license checkout and checkin requests and AutoPass License Server responses. <p>Note: It is recommended to select the Request and Response option.</p>
<p>Borrow Setting</p>	<p>Enables you to instruct the AutoPass License Server to allow license borrowing by other AutoPass License Servers.</p> <p>To prevent a license from borrowing licenses, clear the option.</p> <p>For details on license borrowing, see "Borrowing Licenses" on page 73.</p>
<p>License Pre-Expiry Notification</p>	<p>Enables you to send an advance notification to the AutoPass License Server administrator of approaching product license expirations.</p> <p>If you select this option, you must enter the number of days before expiration on which to send the notification.</p>
<p>Concurrent License Setting</p>	<p>Enables you to retrieve the server details directly from a client request, instead of using the values set in Server Configurations.</p> <p>When this setting is enabled, the protocol type, IP address or host name, and the entry port are identified from the client's request URL. When disabled, the Server Configurations values are used.</p> <p>Default value: Enabled</p>
<p>Server Configurations</p>	<p>Enables you to set the server details for the AutoPass License Server.</p> <p>Enter the following details:</p> <ul style="list-style-type: none"> • Protocol Type: The connection protocol for accessing the License Server. You can select HTTP or HTTPS.

UI Element	Description
	<p>Default: HTTPS</p> <p>Note:</p> <ul style="list-style-type: none"> • APLS is packaged with the RSA 2048 HPE Standard certificate for SSL communication. You can modify the certificate in the server configuration, but we recommend that you use a certificate such as RSA 2048 with SHA 256 to avoid any known security issues. • It is recommended to use certification authority (CA) issued certificate and not self-signed. For more information on installing a certificate refer to "Installing a Certificate from a Certificate Authority" on page 30 <ul style="list-style-type: none"> • IP/Host: The IP address or Host Name of the AutoPass License Server. You can click Search to browse the subnet for available IP addresses or host names. <p>Note: IPv6 addresses must be enclosed with square brackets [].</p> • Port: The entry port for the server. <p>Note: If Concurrent License Setting > Use client settings for checkin/checkout is enabled, the Server Configurations settings are applicable only for Remote Commuter check in and check out. For details, see "Commuter License Check In and Check Out" on page 123.</p> <p>The changes for Server Configurations doesn't reflect in the Web Server Configurations. You should change the settings in the server.xml in the installed relative path \HP\HP AutoPass License Server\HP AutoPass License Server\HP AutoPass License Server\conf</p>
<p>Enable Discovery</p>	<p>Enables you to allow other AutoPass License Servers and clients to discover the AutoPass License Server when searching the subnet to borrow or to check out a license.</p> <p>You can configure the following options:</p> <ul style="list-style-type: none"> • Enable Discover: Allows other AutoPass License Servers and client to find the AutoPass License Server when browsing the subnet. • Excluded Clients: A list of all AutoPass License Servers and client computers that are prevented from finding the AutoPass License Server. Enter a client or AutoPass License Server IP address and click Add to block AutoPass License Server discovery.

SSL Configuration

To install and configure SSL support on Tomcat, you need to follow the below steps.

1. Create a keystore file to store the server's private key and self-signed certificate by executing the following command:

Windows:

```
"%JAVA_HOME%\bin\keytool" -genkey -alias tomcat -keyalg RSA
```

Unix:

`$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA` and specify a password value of "changeit".

2. Uncomment the "SSL HTTP/1.1 Connector" entry in `$CATALINA_BASE/conf/server.xml` and modify as described in the section below.

Prepare the Certificate Keystore

Tomcat currently operates only on JKS, PKCS11 or PKCS12 format keystores. The JKS format is Java's standard "Java KeyStore" format, and is the format created by the keytool command-line utility. This tool is included in the JDK. The PKCS12 format is an internet standard, and can be manipulated via (among other things) OpenSSL and Microsoft's Key-Manager.

Each entry in a keystore is identified by an alias string. Whilst many keystore implementations treat aliases in a case insensitive manner, case sensitive implementations are available. The PKCS11 specification, for example, requires that aliases are case sensitive. To avoid issues related to the case sensitivity of aliases, it is not recommended to use aliases that differ only in case.

To import an existing certificate into a JKS keystore, please read the documentation (in your JDK documentation package) about keytool. Note that OpenSSL often adds readable comments before the key, but keytool does not support that. So if your certificate has comments before the key data, remove them before importing the certificate with keytool.

To import an existing certificate signed by your own CA into a PKCS12 keystore using OpenSSL you would execute a command like:

```
openssl pkcs12 -export -in mycert.crt -inkey mykey.key  
-out mycert.p12 -name tomcat -CAfile myCA.crt  
-caname root -chain
```

For more advanced cases, consult the OpenSSL documentation.

To create a new JKS keystore from scratch, containing a single self-signed Certificate, execute the following from a terminal command line:

Windows:

```
"%JAVA_HOME%\bin\keytool" -genkey -alias tomcat -keyalg RSA
```

Unix:

```
$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA
```

(The RSA algorithm should be preferred as a secure algorithm, and this also ensures general compatibility with other servers and components.)

This command will create a new file, in the home directory of the user under which you run it, named ".keystore". To specify a different location or filename, add the `-keystore` parameter, followed by the complete pathname to your keystore file, to the keytool command shown above. You will also need to reflect this new location in the `server.xml` configuration file, as described later. For example:

Windows:

```
"%JAVA_HOME%\bin\keytool" -genkey -alias tomcat -keyalg RSA
```

-keystore \path\to\my\keystore

Unix:

\$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA

-keystore /path/to/my/keystore

After executing this command, you will first be prompted for the keystore password. The default password used by Tomcat is "changeit" (all lower case), although you can specify a custom password if you like. You will also need to specify the custom password in the server.xml configuration file, as described later.

Next, you will be prompted for general information about this Certificate, such as company, contact name, and so on. This information will be displayed to users who attempt to access a secure page in your application, so make sure that the information provided here matches what they will expect.

Finally, you will be prompted for the key password, which is the password specifically for this Certificate (as opposed to any other Certificates stored in the same keystore file). You **MUST** use the same password here as was used for the keystore password itself. This is a restriction of the Tomcat implementation. (Currently, the keytool prompt will tell you that pressing the ENTER key does this for you automatically.)

If everything was successful, you now have a keystore file with a Certificate that can be used by your server.

Note: Your private key password and keystore password should be the same. If they differ, you will get an error along the lines of java.io.

Edit the Tomcat Configuration File

Tomcat can use two different implementations of SSL:

- The JSSE implementation provided as part of the Java runtime (since 1.4)
- The APR implementation, which uses the OpenSSL engine by default.

The exact configuration details depend on which implementation is being used. If you configured Connector by specifying generic protocol="HTTP/1.1" then the implementation used by Tomcat is chosen automatically. If the installation uses APR - i.e. you have installed the Tomcat native library - then it will use the APR SSL implementation, otherwise it will use the Java JSSE implementation.

As configuration attributes for SSL support significantly differ between APR vs. JSSE implementations, it is recommended to avoid auto-selection of implementation. It is done by specifying a classname in the protocol attribute of the Connector.

To define a Java (JSSE) connector, regardless of whether the APR library is loaded or not, use one of the following:

```
<!-- Define a HTTP/1.1 Connector on port 8443, JSSE BIO implementation -->
```

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
```

```
port="8443" .../>
```

```
<!-- Define a HTTP/1.1 Connector on port 8443, JSSE NIO implementation -->
```

```
<Connector protocol="org.apache.coyote.http11.Http11NioProtocol"
```

```
port="8443" .../>
```

Alternatively, to specify an APR connector (the APR library must be available) use:

```
<!-- Define a HTTP/1.1 Connector on port 8443, APR implementation -->
<Connector protocol="org.apache.coyote.http11.Http11AprProtocol"
port="8443" .../>
```

If you are using APR, you have the option of configuring an alternative engine to OpenSSL.

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="someengine" SSLRandomSeed="somedevice" />
```

The default value is

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" SSLRandomSeed="builtin" />
```

So to use SSL under APR, make sure the SSLEngine attribute is set to something other than off. The default value is on and if you specify another value, it has to be a valid engine name.

SSLRandomSeed allows to specify a source of entropy. Productive system needs a reliable source of entropy but entropy may need a lot of time to be collected therefore test systems could use no blocking entropy sources like "/dev/urandom" that will allow quicker starts of Tomcat.

The final step is to configure the Connector in the \$CATALINA_BASE/conf/server.xml file, where \$CATALINA_BASE represents the base directory for the Tomcat 6 instance. An example <Connector> element for an SSL connector is included in the default server.xml file installed with Tomcat. For JSSE, it should look something like this:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector
protocol="org.apache.coyote.http11.Http11Protocol"
port="8443" maxThreads="200"
scheme="https" secure="true" SSLEnabled="true"
keystoreFile="{user.home}/.keystore" keystorePass="changeit"
clientAuth="false" sslProtocol="TLS"/>
```

The APR connector uses different attributes for many SSL settings, particularly keys and certificates. An example of an APR configuration is:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector
protocol="org.apache.coyote.http11.Http11AprProtocol"
port="8443" maxThreads="200"
scheme="https" secure="true" SSLEnabled="true"
SSLCertificateFile="/usr/local/ssl/server.crt"
SSLCertificateKeyFile="/usr/local/ssl/server.pem"
SSLVerifyClient="optional" SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"/>
```

The configuration options and information on which attributes are mandatory for the JSSE based connectors (BIO and NIO) are documented in the SSL Support section of the HTTP connector configuration reference. The configuration options and information on which attributes are mandatory for the APR connector are documented in the HTTPS section of the APR How-To.

The port attribute is the TCP/IP port number on which Tomcat will listen for secure connections. You can change this to any port number you wish (such as to the default port for https communications, which is 443). However, special setup (outside the scope of this document) is necessary to run Tomcat on port numbers lower than 1024 on many operating systems.

If you change the port number here, you should also change the value specified for the redirectPort attribute on the non-SSL connector. This allows Tomcat to automatically redirect users who attempt to access a page with a security constraint specifying that SSL is required, as required by the Servlet Specification.

After completing these configuration changes, you must restart Tomcat as you normally do, and you should be in business. You should be able to access any web application supported by Tomcat via SSL. For example, try:

https://localhost:8443/

and you should see the usual Tomcat splash page (unless you have modified the ROOT web application).

SMTP Mail Configuration

Simple Mail Transfer Protocol (SMTP) communications servers use transport-layer security (TLS) or SSL encryption which provides privacy and authentication. The mail configuration secures the SMTP sessions using the STARTTLS property mentioned below in **mailconfig.properties** file in the path

\\HP\HP AutoPass License Server\AutoPass\LicenseServer\data\conf\.

“mail.smtp.starttls.enable” = true

Note: Configuring SMTP is mandatory if the password has to be reset.

Installing a Certificate from a Certificate Authority

To obtain and install a Certificate from a Certificate Authority (like verisign.com, thawte.com or trustcenter.de), read the previous section and then follow these instructions:

Create a local Certificate Signing Request (CSR)

In order to obtain a Certificate from the Certificate Authority of your choice you have to create a so called Certificate Signing Request (CSR). That CSR will be used by the Certificate Authority to create a Certificate that will identify your website as "secure". To create a CSR follow these steps:

Create a local self-signed Certificate (as described in the previous section):

keytool -genkey -alias tomcat -keyalg RSA

-keystore <your_keystore_filename>

Note: In some cases you will have to enter the domain of your website (i.e. www.myside.org) in the field "first- and lastname" in order to create a working Certificate.

The CSR is then created with:

```
keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr
```

```
-keystore <your_keystore_filename>
```

Now you have a file called certreq.csr that you can submit to the Certificate Authority (look at the documentation of the Certificate Authority website on how to do this). In return you get a Certificate.

Importing the Certificate

Now that you have your Certificate you can import it into your local keystore. First of all you have to import a so called Chain Certificate or Root Certificate into your keystore. After that you can proceed with importing your Certificate.

- Download a Chain Certificate from the Certificate Authority you obtained the Certificate from.

For Verisign.com commercial certificates go to:

<http://www.verisign.com/support/install/intermediate.html>

For Verisign.com trial certificates go to: http://www.verisign.com/support/verisign-intermediate-ca/Trial_Secure_Server_Root/index.html

For Trustcenter.de go to: <http://www.trustcenter.de/certservices/cacerts/en/en.htm#server>

For Thawte.com go to: <http://www.thawte.com/certs/trustmap.html>

- Import the Chain Certificate into your keystore

```
keytool -import -alias root -keystore <your_keystore_filename>
```

```
-trustcacerts -file <filename_of_the_chain_certificate>
```

- And finally import your new Certificate

```
keytool -import -alias tomcat -keystore <your_keystore_filename>
```

```
-file <your_certificate_filename>
```

AutoPass License Server Configuration - Frequently Asked Questions

Why did the Mail Configuration page open as the start up page when I logged into the AutoPass License Server?

The Mail Configuration settings are required during the first login to the AutoPass License Server.

Where does the AutoPass License Server store the audit log file?

The log file is found at <Your data directory>\Autopass\LicenseServer\data\log>.

How do I change the HPE AutoPass License Server .log file location?

To change the .log file location, modify the log4j.properties file located at <Your data directory>\Autopass\LicenseServer\data\conf>.

To change the .log file location, make sure that the following information is entered into the .log4j.properties file:

```
log4j.logger.com.hp.autopassj=INFO,APJ
log4j.appender.APJ=org.apache.log4j.RollingFileAppender
log4j.appender.APJ.File=<log file path>\\autopassls.log
log4j.appender.APJ.MaxFileSize=10MB
log4j.appender.APJ.MaxBackupIndex=10
log4j.appender.APJ.Append=True
log4j.appender.APJ.layout=org.apache.log4j.PatternLayout
log4j.appender.APJ.layout.ConversionPattern=%-5p- %d{MMM dd HH:mm:ss} - %m%n
```

Note: You need to restart the AutoPass License Server in order for the changes to take effect.

How do I change the AutoPass License Server .log file size?

To change the .log file size, modify the log4j.properties file located at <Your data directory>\Autopass\LicenseServer\data\conf>.

To change the .log file location, make sure that the following information is entered into the .log4j.properties file:

```
log4j.logger.com.hp.autopassj=INFO,APJ
log4j.appender.APJ=org.apache.log4j.RollingFileAppender
log4j.appender.APJ.File=<Provide the log file path here>\\autopassls.log
log4j.appender.APJ.MaxFileSize=<log file size>
log4j.appender.APJ.MaxBackupIndex=10
log4j.appender.APJ.Append=true
log4j.appender.APJ.layout=org.apache.log4j.PatternLayout
log4j.appender.APJ.layout.ConversionPattern=%-5p - %d{MMM dd HH:mm:ss} - %m%n
```

Note: You need to restart the AutoPass License Server in order for the changes to take effect.

If I disable the Borrow option after another AutoPass License Server has borrowed licenses, can the borrowing AutoPass License Server return the licenses?

Yes.

How do I prevent another AutoPass License Server or a client machine from detecting this AutoPass License Server?

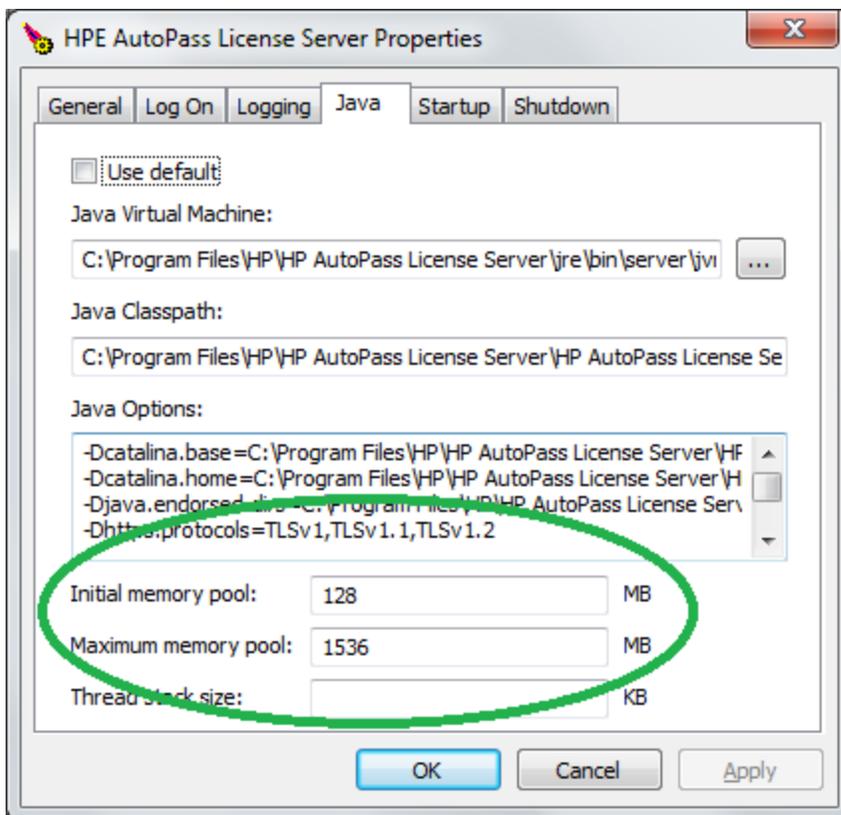
In the Main tab (Configuration pane), enter the AutoPass License Server's or client's IP address and click **Add**. The client user or AutoPass License Server is added to the list of Excluded Clients and cannot discover the AutoPass License Server.

How do I increase Java heap memory size?

To change the Java heap memory, modify the hpLicSvrw.exe file located in <Your installation directory>\HP \bin>.

To modify the memory, do the following:

1. Double-click on the hpLicSvrw.exe file.
2. Select the **Java** tab.
3. In the **Maximum memory pool** field, enter the amount of memory you want.



Note: The maximum amount of memory allowed is 1408 MB.

4. Restart the AutoPass License Server.

Chapter 6: Integration with HP Usage Hub

This chapter includes:

Concepts

- ["Usage Hub Configuration Overview" on the next page](#)

Reference

- ["Usage Hub Server Tab \(Configuration Pane\)" on page 36](#)
- ["Usage Hub Configuration - Frequently Asked Questions" on page 38](#)

Concepts

Usage Hub Configuration Overview

If you have HP Usage Hub running in your environment, AutoPass License Server can report usage data to the Hub server.

Follow the steps below to set configuration options for Usage Hub Server.

- Usage Hub IP/Host Name
- Changing Usage Hub default credentials
- Enabling/Disabling Usage Data Reporting
- Data Synchronization Interval with Hub

For details about the individual options, see [Usage Hub Server Tab \(Configuration Pane\)](#)

Reference

Usage Hub Server Tab (Configuration Pane)

The Usage Hub Server tab enables you to configure Usage HubAutoPass License Server settings.

|

To access	Configuration pane > Usage Hub Server tab
Important information	This tab is enabled only if Usage Hub Connector is checked in the Main Configuration tab.

UI Element	Description
<p>Usage Collection and Communication Configurations</p>	<p>Enables you to configure the settings for usage hub data collection and communication with License Server</p> <p>You can enter the following details:</p> <ul style="list-style-type: none"> • Usage Hub IP/Host Name The IP/Host name of the server to which the license usage data is pushed to. <i>(required field)</i> • Test Connection: The IP/Hostname connection can be tested. Click Test Connection after entering a IP/Hostname. • Change Default User Credentials for Hub: Enter the valid username and password, if default credentials of Usage Hub needs to be changed. <p>Note: The credentials should match usage hub web service user.</p> <ul style="list-style-type: none"> • Disable Usage Data Reporting: Allows you to disable usage data reporting. • Data Synchronization Interval With Hub: The usage data of licenses with License Server and Usage Hub can be synchronized in regular intervals which is configurable. Enter the values in minutes.

Usage Hub Configuration - Frequently Asked Questions

Why are the rejected requests not captured by Usage Hub?

It is because the maximum rejected requested capacity will not be tracked if reservation is set and capacity requested is more than the reserved capacity.

How is usage captured in redundancy mode?

Usage is sent by primary and secondary servers individually. Secondary will capture usage data only when primary is down.

Chapter 7: AutoPass License Server Redundancy Configuration

This chapter includes:

Concepts

- ["AutoPass License Server Redundancy - Overview" on the next page](#)
- ["AutoPass License Server Redundancy - Considerations and Limitations" on the next page](#)

Tasks

- ["How to Configure AutoPass License Server Redundancy" on page 42](#)

Reference

- ["Redundancy Tab \(Configuration Pane\)" on page 44](#)
- ["AutoPass License Server Redundancy - Frequently Asked Questions" on page 46](#)
- ["AutoPass License Server Redundancy - Troubleshooting and Limitations" on page 47](#)

Concepts

AutoPass License Server Redundancy - Overview

After you install and configure your AutoPass License Server, you can configure server redundancy for a AutoPass License Server. **Server redundancy**¹ is the practice of having a secondary server prepared as a backup to a primary server. This secondary server is operational only when the primary server is unavailable.

By default, each AutoPass License Server is considered a standalone server immediately after installation. However, each AutoPass License Server can support an additional AutoPass License Server to serve as a redundant server.

When both the primary and secondary AutoPass License Servers are operational, the data in both AutoPass License Servers is automatically synchronized.

When you configure redundancy in a pair of AutoPass License Servers, the primary AutoPass License Server controls the operation of all AutoPass License Server functions, and defines all configuration settings and information. For example, the configuration settings from the primary server are in effect, regardless of any configuration changes made on the secondary server. Any attempts to access the secondary AutoPass License Server via a Web browser are redirected to the primary AutoPass License Server.

If the license of the primary AutoPass License Server expires, server redundancy is not active and the secondary AutoPass License Server does not function in place of the primary AutoPass License Server. In this case, client users cannot check out licenses and checked out licenses cannot be renewed. Likewise, licenses cannot be checked out or renewed if the primary AutoPass License Server is not operational and the secondary AutoPass License Server license expires.

Note: Client users can still check in licenses into an expired AutoPass License Server, regardless of redundancy status or availability.

AutoPass License Server Redundancy - Considerations and Limitations

When configuring redundancy, note the following:

- Both the primary and secondary AutoPass License Servers must be the same server version.
- You must configure the secondary AutoPass License Server before configuring the primary AutoPass License Server. For task details, see "[How to Configure AutoPass License Server Redundancy](#)" on page 42
- A primary AutoPass License Server can have only one secondary AutoPass License Server.

¹The configuration in which a backup server is prepared in the event of a failure or unavailability of the primary server.

- A secondary AutoPass License Server cannot be shared with more than one primary AutoPass License Server.
- A AutoPass License Server acting as the primary AutoPass License Server should have a license for the secondary AutoPass License Server.
- If you configure a standalone AutoPass License Server as a primary AutoPass License Server, only the licenses installed on the standalone server are maintained when the server becomes a primary AutoPass License Server. Installed active licenses will be retained once primary server is setup, other information from the stand alone server is cleared. You must update all other configuration settings.

Tasks

How to Configure AutoPass License Server Redundancy

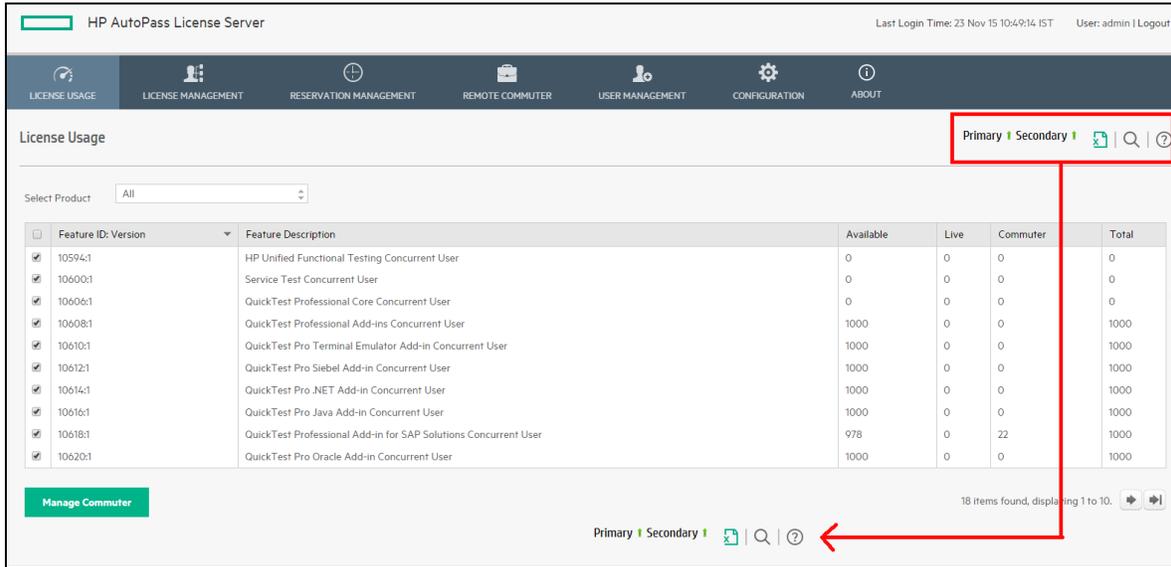
This task describes how to configure server redundancy for the AutoPass License Server.

1. In the secondary AutoPass License Server, in the Redundancy Tab (Configuration Pane), select the **Enable Redundancy** option check box and the **Act as Secondary** option check box.
2. Enter the **Local IP** address in the edit box for the current AutoPass License Server. If you want to search the subnet for available IP addresses, click **Select** to list all available IP addresses and select an address from the search box.
3. In the primary AutoPass License Server, install the licenses for the primary and the secondary AutoPass License Servers.

Note: The licenses for the primary and secondary servers should be locked to the primary IP address of the primary AutoPass License Server.

4. In the primary AutoPass License Server, in the Redundancy Tab (Configuration Pane), select the **Enable Redundancy** option check box.
5. Select the **Protocol Type**.
6. Enter the **Local IP**, the **Redundant IP**, the **Redundant Port**, and the **Protocol Port** for the secondary AutoPass License Server. For details on these options, see "[Redundancy Tab \(Configuration Pane\)](#)" on page 44.
7. Click **Save**.

After redundancy is configured, the server status is displayed in the License Usage pane, as seen in the example below.



If a server is operational, it is represented by a green arrow pointing upward. If a server is not operational, it is represented with a red arrow pointing downward. If the primary and secondary AutoPass License Servers are represented by green arrows pointing upward, the primary AutoPass License Server is handling the server operations.

Note: If you need to change the secondary AutoPass License Server defined for a primary AutoPass License Server, you must first configure the primary AutoPass License Server as a standalone AutoPass License Server by clearing the Enable Redundancy option. After saving this configuration change, you may then configure the now standalone AutoPass License Server as a primary AutoPass License Server with a different secondary AutoPass License Server.

Reference

Redundancy Tab (Configuration Pane)

This tab enables you to configure AutoPass License Server redundancy.

The screenshot shows the 'Redundancy Configuration' pane with the following settings:

- Enable Redundancy:
- Act as Secondary:
- Local IP: select
- Redundant IP:
- Redundant Port:
- Protocol Type:
- Protocol Port:

Buttons: Save (green), Cancel (grey)

To access	Configuration pane > Redundancy tab
Important information	Each primary AutoPass License Server can have only one secondary AutoPass License Server.
Relevant tasks	"How to Configure AutoPass License Server Redundancy" on page 42
See also	<ul style="list-style-type: none">• "AutoPass License Server Redundancy - Overview" on page 40• "AutoPass License Server Redundancy - Considerations and Limitations" on page 40

User interface elements are described below:

UI Element	Description
Enable Redundancy	Enables the AutoPass License Server to serve as a primary or secondary AutoPass License Server.
Act as Secondary	Enables the AutoPass License Server to serve as the secondary AutoPass License Server for the primary AutoPass License Server defined in the IP settings.
Local IP	The IP address of the same AutoPass License Server (the primary AutoPass License Server if configuring a primary server or the secondary AutoPass License Server if configuring a secondary server).
Select	Displays the Local IP address of the AutoPass License Server.
Redundant IP	<p>The IP address for the secondary AutoPass License Server.</p> <p>Note: This option is available only when configuring the primary AutoPass License Server.</p>
Redundant Port	<p>The port on which the internal database of the secondary AutoPass License Server listens to synchronize the data between the primary and secondary AutoPass License Servers.</p> <p>Note: This option is available only when configuring the primary AutoPass License Server.</p>
Protocol Type	<p>The connection protocol for connecting to the partner AutoPass License Server: UDP (default) or TCP</p> <p>Note: If the primary and secondary servers are located in the same subnet, it is recommend to use the <i>UDP</i> protocol. If the servers are on different subnets, you should use the <i>TCP</i> protocol.</p>
Protocol Port	The port on which the primary and secondary AutoPass License Servers communicate to exchange their status.

AutoPass License Server Redundancy - Frequently Asked Questions

How can I disable redundancy for a specific primary or secondary AutoPass License Server?

In the Redundancy tab (Configuration pane), clear the **Enable Redundancy** check box.

How do I define a AutoPass License Server as a primary AutoPass License Server?

In the Redundancy tab (Configuration pane), select the **Enable Redundancy** option check box and provide the details for the secondary server, as described in ["How to Configure AutoPass License Server Redundancy" on page 42](#). For details on the Redundancy tab, see ["Redundancy Tab \(Configuration Pane\)" on page 44](#).

How do I define a AutoPass License Server as a secondary AutoPass License Server?

In the Redundancy tab (Configuration pane), select the **Enable Redundancy** option check box and the **Act as Secondary** option checkbox. Provide the details for the primary server, as described in ["How to Configure AutoPass License Server Redundancy" on page 42](#). For details on the Redundancy tab, see ["Redundancy Tab \(Configuration Pane\)" on page 44](#).

AutoPass License Server Redundancy - Troubleshooting and Limitations

Why can I not connect to the secondary AutoPass License Server when the primary AutoPass License Server is down, even after I have configured both AutoPass License Servers?

You must ensure that both the **Redundant Port** and **Protocol Port** on both AutoPass License Servers are open. If one or both of the ports are closed on either of the servers, the automatic communication and data synchronization does not work.

Chapter 8: AutoPass License Server User and User Group Management

This chapter includes:

Concepts

- ["AutoPass License Server Users - Overview" on the next page](#)
- ["AutoPass License Server User Groups - Overview" on the next page](#)
- ["User Group Privilege Levels" on the next page](#)
- ["AutoPass License Server User Group Privilege Matrix" on page 50](#)
- ["User and User Group Sources" on page 51](#)

Tasks

- ["How to Manage AutoPass License Server Users and User Groups" on page 53](#)

Reference

- ["Users Tab \(User Management Pane\)" on page 57](#)
- ["User Groups Tab \(User Management Pane\)" on page 59](#)
- ["User Management Tab \(Configuration Pane\)" on page 62](#)
- ["LDAP Tab \(Configuration Pane\)" on page 65](#)

["AutoPass License Server User and User Group Management - Frequently Asked Questions" on page 67](#)

["AutoPass License Server User and User Group Management - Troubleshooting and Limitations" on page 69](#)

Concepts

AutoPass License Server Users - Overview

After initially configuring the AutoPass License Server, you create **administrative users**¹ responsible for the creation and maintenance of licenses and client users. AutoPass License Server users, unlike client users, have access to the AutoPass License Server functionality to ensure the running and operation of the AutoPass License Server.

By default, the AutoPass License Server has one user, named *admin* (which is used to log in to the AutoPass License Server the first time). On the initial login to the AutoPass License Server, you log in using the *admin* user. However, after logging in once, you can create additional users and assign them specific roles and privileges for using the AutoPass License Server.

For details on how to create users, see ["How to Manage AutoPass License Server Users and User Groups" on page 53](#).

AutoPass License Server User Groups - Overview

After you create administrative users, you also create user groups. These user groups enable you to group administrative users in a way suited to your organization and license usage.

Example

You create 16 new users for your AutoPass License Server. These 16 users are responsible for administering the licenses of four different products. Each product has 4 users, who rotate administrative responsibility throughout the day. Using the user groups, you can group each group of four users together to ensure easier and more visible organization of the users.

However, in addition to helping you organize AutoPass License Server users, you can use user groups to administer AutoPass License Server access privileges. Depending on a user's group and the corresponding privilege levels, the user has varying access privileges which enable or prevent the user from performing certain administrative tasks. For details, see ["User Group Privilege Levels" below](#).

For details on creating and managing user groups, see ["How to Manage AutoPass License Server Users and User Groups" on page 53](#).

User Group Privilege Levels

For each user group (and by extension, each user), you assign a specific privilege level. The access privilege level determines the access level to various AutoPass License Server tasks.

Note: You cannot assign a privilege level directly to a user.

¹A user created in the License Server responsible for administering the License Server.

You can assign any of the following access privilege levels to a group:

- **Administrator:** Users with this access privilege level are given full permissions to perform all AutoPass License Server tasks.
- **Product Admin:** Users with this access privilege level are given full permissions to install and maintain licenses for products to which they are assigned. They cannot perform general AutoPass License Server administrative tasks, including AutoPass License Server configuration and user and user group management tasks.
- **View-Only:** Users with this access privilege are allowed to view license information. They cannot perform general AutoPass License Server administrative tasks.

By default, any new user group is created with the *View-Only* access permission. You can modify this access privilege level later if needed. For details, see ["User Groups Tab \(User Management Pane\)" on page 59](#).

All users not added to a user group are given *View-Only* permissions.

For additional details about the specific tasks permitted for each access privilege level, see ["AutoPass License Server User Group Privilege Matrix" below](#).

For details on creating and modifying user group privilege levels, see ["Set user group access privileges" on page 55](#).

AutoPass License Server User Group Privilege Matrix

This table specifies the ability to perform various AutoPass License Server operations based on user group access privileges. For details on setting access privileges, see [Set user group access privileges](#).

Functionality	Administrator	Product Admin	View Only
Manage Commuter	Yes	Yes*	No
Feature Report	Yes	Yes	Yes
Export Feature Report	Yes	Yes	Yes
Download Commuter/Remote Commuter License Details	Yes	Yes*	No
Search Result Report	Yes	Yes	Yes
Revoke	Yes	Yes*	No
Purge	Yes	No	No
Install License	Yes	Yes	Yes
License Management	Yes	Yes	Yes

Functionality	Administrator	Product Admin	View Only
Export License Details to Excel	Yes	Yes	Yes
Archive Licenses	Yes	Yes*	No
Manage Archived License	Yes	Yes*	No
Borrow License	Yes	Yes*	No
View Checked-In History	Yes	Yes	Yes
Delete/Return the archived licenses	Yes	Yes*	No
License Clean-up	Yes	Yes*	No
Creating a Pool	Yes	Yes	Yes
Mapping feature to a pool	Yes	Yes*	No
Mapping product to a pool	Yes	Yes*	No
Remote commuter check-out	Yes	Yes*	No
Remote commuter check-in	Yes	Yes	Yes
User Management	Yes	No	No
Configuration	Yes	No	No

* Privilege is limited to the product assigned to the product administrator user.

User and User Group Sources

When you create users and user groups, you can choose to store user and user group information in the following locations:

- **AutoPass License Server internal database:** All user and user group information is stored locally with the AutoPass License Server and you can create, modify, and delete data from the database.
- **LDAP database:** All user and user group information is stored on an external LDAP server. You import the users and/or user groups from the LDAP server into the AutoPass License Server. You cannot create, modify, or delete data from the LDAP server from within the AutoPass License Server.

After importing user and user groups from an LDAP server, you cannot modify user information, or add or delete users, as these are stored on the LDAP server. However, you can add users that are imported from an LDAP server to user groups stored on the AutoPass License Server's internal database and grant those users privilege levels.

Note: If you import user groups from the LDAP server, you cannot add users created and stored in

the AutoPass License Server internal database.

For information on configuring LDAP connection, see "[LDAP Tab \(Configuration Pane\)](#)" on page 65.

Tasks

How to Manage AutoPass License Server Users and User Groups

This task describes the procedures necessary to create and maintain AutoPass License Server administrative users and user groups.

This task includes the following steps:

- ["Create a user" below](#)
- ["Modify a user's status" on the next page](#)
- ["Update user details" on the next page](#)
- ["Reset a user's password" on the next page](#)
- ["Add a user to existing user groups" on the next page](#)
- ["Add a new user group" on page 55](#)
- ["Update group details" on page 55](#)
- ["Set user group access privileges" on page 55](#)
- ["Import groups from an LDAP server" on page 55](#)
- ["Associate products with a Product Admin group" on page 56](#)

Create a user

1. In the Users tab (User Management pane), click  button.
2. In the Create New User dialog box, enter the first and last name of the user and the user's email address.

Note: You must enter a valid e-mail address because the AutoPass License Server sends a message containing the user's password details to the address listed.

3. Click **Create**.

A new user is added to the users table in the upper pane of the Users Tab. The user's details are displayed in the lower pane.

Modify a user's status

1. In the upper pane of the Users tab (User Management pane), select the radio button for the user whose status you want to update.
2. In the lower pane, click the **Change Status** link.

The user's status changes in the lower pane (to *active* or *inactive*).

Note: If a user is listed as *inactive*, the user is unable to log in to the AutoPass License Server.

Update user details

1. In the upper pane of the Users tab (User Management pane), select the radio button for the user whose status you want to update.
2. In the lower pane, enter the modified details in the relevant edit boxes.

Note: You can update the email address only for the default administrator.

3. Click **Save**.

The new details are displayed in the user table in the upper pane of the Users tab.

Note: You can also modify a user's details by clicking the **<user name>** link at the top of the AutoPass License Server window after logging in as the user.

Reset a user's password

1. In the upper pane of the Users tab (User Management pane), select the radio button for the user whose password you want to reset.
2. In the lower pane, click the **Reset Password** link.

The user's password is reset and an e-mail message is sent with the new password to the address defined in the lower pane.

Note: You can also reset a user password by entering a user's login name and clicking the **Forgot Password** link on the AutoPass License Server login page.

Add a user to existing user groups

1. In the upper pane of the Users tab (User Management pane), select the radio button for the user you want to add to a user group.
2. In the lower pane, click the **Search** button . The Assign Groups dialog box opens.
3. In the Assign Groups dialog box, select the check box for any group to which you want to add the user.
4. Click **Add**.

The selected groups are added to the Associated User Groups list in the lower pane of the Users tab.

Note: To remove a user from a group, click the **Delete** button  next to the group name.

Add a new user group

1. In the User Groups tab (User Management pane), click **+** button.
2. In the Create New Group dialog box, enter the **Group Name**, **Description**, and **Group Email**.
3. If you want this group to have administrator access privileges, select the **Mark as administrator** option.
4. Click **Create**.

A new user group is added to the table in the upper pane of the User Groups tab and the group details are displayed in the lower pane.

Update group details

1. In the upper pane of the User Groups tab (User Management pane), select the radio button for the user group whose status you want to update.
2. In the lower pane, enter the modified details in the relevant edit boxes.
3. Click **Save**.

The new details are displayed in the User Groups table in the User Groups tab.

Set user group access privileges

1. In the upper pane of the User Groups tab (User Management tab), select the radio button of the user for which you want to set access privileges.
2. In the lower pane, in the Manage User Groups tab, select the access privilege level.
3. Click **Save**.

The Manage User Groups tab displays the correct access privilege level and the privilege level details.

Note: By default, all user groups are initially assigned as **View Only**.

Import groups from an LDAP server

1. In the User Management tab (Configuration pane), select **LDAP** as the source for users and user groups. For details, see "[User Management Tab \(Configuration Pane\)](#)" on page 62
2. Click **Save**.
3. In the LDAP tab (Configuration pane), enter the details for your LDAP server. For details, see "[LDAP Tab \(Configuration Pane\)](#)" on page 65.
4. Click **Save**.

The users and/or user groups are added to the Users tab and User Groups tab in the User Management pane.

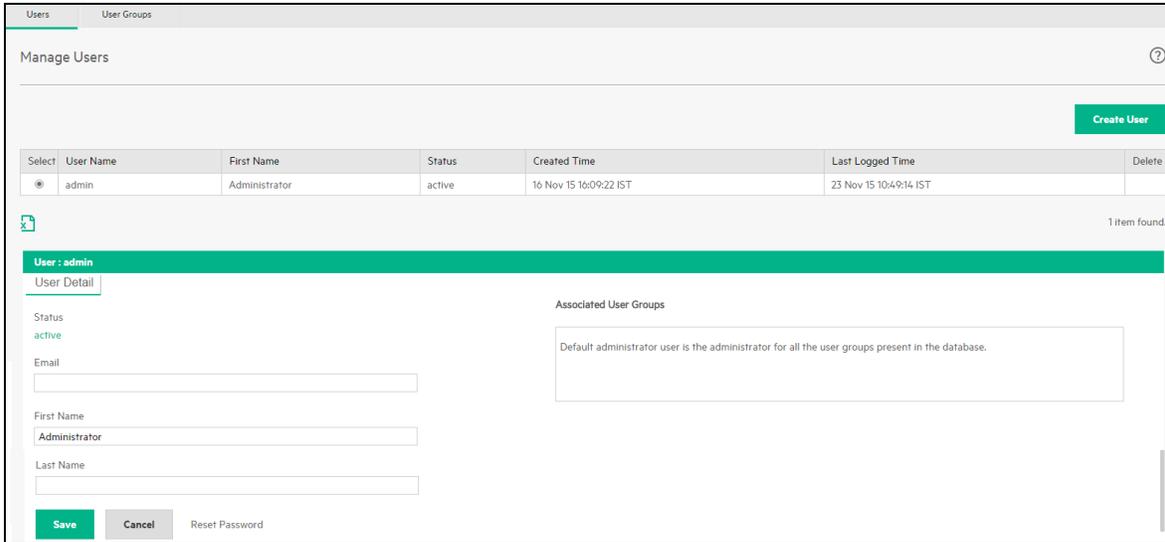
Associate products with a Product Admin group

1. In the User Groups tab (User Management pane), select the Product Admin group to which you want to associate products.
2. In the Manage User Groups tab (lower pane of the Users tab), click the **Search** button . The Assign Products dialog box opens.
3. In the Assign Products dialog box, select the products for this group and click **Add**.
The products for this group are displayed in the Associated Products list in the Manage User Groups tab.

Reference

Users Tab (User Management Pane)

This tab enables you to add administrative users to the AutoPass License Server, add and maintain user details, and add users to user groups.



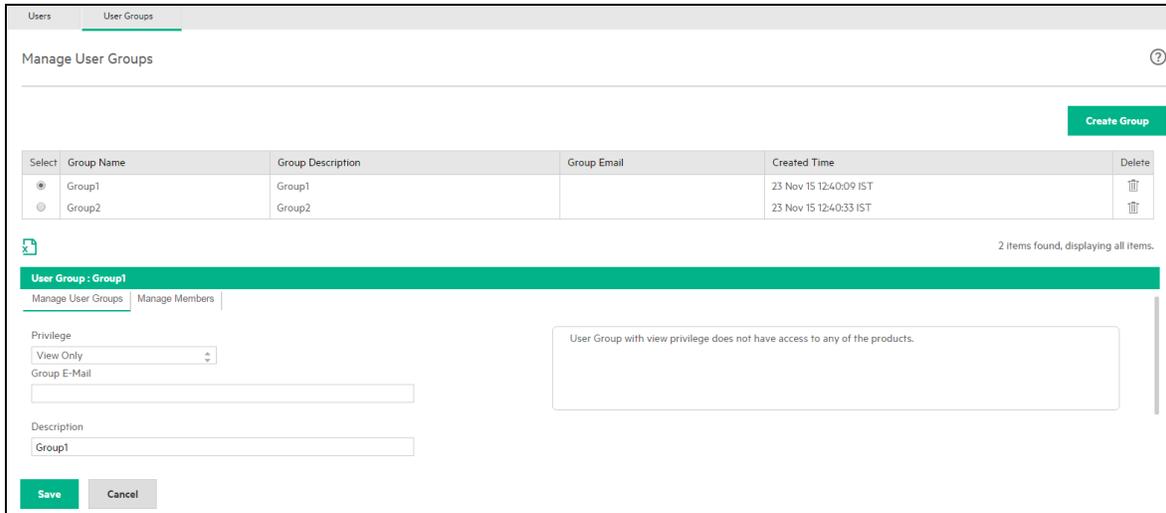
To access	User Management pane > Users tab
Important information	<ul style="list-style-type: none"> You can also update user credentials when logged into the AutoPass License Server by clicking the <user name> link at the top of the AutoPass License Server window. Before you create a new user, ensure that the mail server is configured. For details, see "Mail Configuration" on page 24.
Relevant tasks	<ul style="list-style-type: none"> "Create a user" on page 53 "Modify a user's status" on page 54 "Update user details" on page 54 "Reset a user's password" on page 54 "Add a user to existing user groups" on page 54
See also	"AutoPass License Server Users - Overview" on page 49

User interface elements are described below:

UI Element	Description
	<p>Create User. Opens the Create New User dialog box, enabling you to enter details for a user.</p>
<p>User name</p>	<p>The user name used to log into the AutoPass License Server.</p> <p>Note: The user name displayed in the user table in the Users tab is the email address entered in the Create New User dialog box.</p>
<p>First Name</p>	<p>The user's first name, as entered in the Create New User dialog box.</p>
<p>Status</p>	<p>The user status: <i>active</i> or <i>inactive</i>.</p> <p>Users with an <i>inactive</i> status cannot log in to the AutoPass License Server.</p>
<p>Created Time</p>	<p>The date and time the user was created.</p>
<p>Last Logged Time</p>	<p>The date and time that the user's last logged in to the AutoPass License Server.</p>
	<p>Delete. Removes the user from the AutoPass License Server database.</p> <p>Note: If you import users from an LDAP server, clicking Delete only removes them from the AutoPass License Server's internal database. It does not delete them from the LDAP server.</p>
	<p>Export to Excel. Exports the currently displayed report to Excel.</p>
<p>Email</p>	<p>The user's email address, as entered in the Create New User dialog box.</p>
<p>Reset Password</p>	<p>Resets the users password. An e-mail message is sent to the user with the new user details.</p>
<p>Associated User Groups</p>	<p>The groups to which the selected user belongs.</p>
	<p>Search. Opens the Assign User Groups dialog box, enabling you to assign the user to user groups.</p>
	<p>Removes the user from a user group.</p> <p>Note: Clicking this button in the Associated User Groups list does not remove the user from the AutoPass License Server.</p>

User Groups Tab (User Management Pane)

This tab enables you to create user groups, set access privilege levels, and add users to user groups.



To access	User Management pane > User Groups tab
Important information	Before you create a new user group, ensure that the mail server is configured. For details, see "Mail Configuration" on page 24 .
Relevant tasks	<ul style="list-style-type: none"> • "Add a new user group" on page 55 • "Update group details" on page 55 • "Set user group access privileges" on page 55
See also	<ul style="list-style-type: none"> • AutoPass License Server User Groups - Overview • User Group Privilege Levels • AutoPass License Server User Group Privilege Matrix

User interface elements are described below:

User Groups Table

UI Element	Description
	<p>Create Group. Opens the Create New User Group dialog box, enabling you to enter details for and create a new user group.</p>
<p>Group Name</p>	<p>The name for the group, as entered in the Create New User Group dialog box.</p>
<p>Group Description</p>	<p>The description of the group, as entered in the Create New User Group dialog box.</p>
<p>Group Email</p>	<p>The group email address, as entered in the Create New User Group dialog box.</p> <p>Note: When a new user group is created or deleted, an e-mail message is sent to this address.</p>
<p>Created Time</p>	<p>The date and time of the group's creation.</p>
<p></p>	<p>Delete. Removes the selected user group from the AutoPass License Server internal database.</p> <p>Note: If you imported a user group from an LDAP server, clicking Delete does not remove the user group from the LDAP server.</p>
<p></p>	<p>Export to Excel. Exports the currently selected report to Excel.</p>

Manage User Groups tab

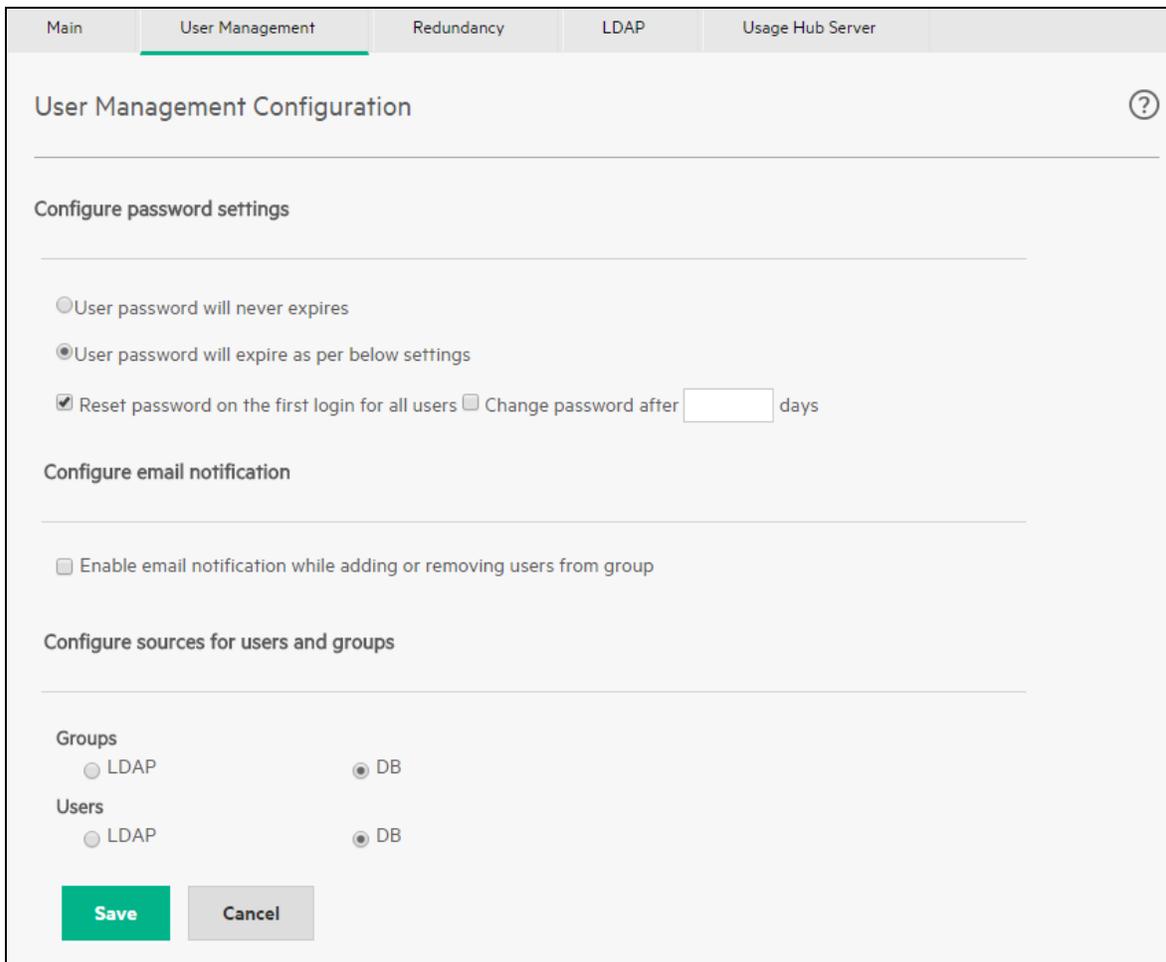
UI Element	Description
Privilege	<p>The access privilege level of the selected group.</p> <p>Each group can have one of three privilege levels:</p> <ul style="list-style-type: none"> • Administrator • Product Admin • View-Only <p>The default level for a user group is <i>View-Only</i>.</p> <p>For details on the privileges for each type of user, see "User Group Privilege Levels" on page 49.</p>
Associated Products (for Product Admin groups only)	<p>The products associated with the selected user group.</p> <p>A user group with Product Admin privilege levels has access privileges only for products listed in this window.</p>
	<p>Search. Opens the Assign Products dialog box, enabling you to associate a <i>Product Admin</i> group with currently configured products.</p>
	<p>Delete. Removes a product from association with a <i>Product Admin</i> user group.</p>
Group Description	<p>The description of the group, as entered in the Create New User Group dialog box.</p>
Group Email	<p>The group email address, as entered in the Create New User Group dialog box.</p>

Manage Members Tab

UI Element	Description
<user name>	Enables you to search the users by name in order to add them to a particular user group.
	Opens the Assign Users dialog box, enabling you to select which users to add to a user group. Note: The Assign Users dialog box contains all AutoPass License Server users.
<associated users list>	The list of all users added to the user group.
	Remove. Removes a member from a user group. Note: Clicking Remove in this tab does not delete the user.

User Management Tab (Configuration Pane)

This tab enables you to set configuration settings for users and user groups.



To access	Configuration pane > User Management tab
Relevant tasks	<ul style="list-style-type: none"> • "Reset a user's password" on page 54 • "Import groups from an LDAP server" on page 55
See also	"User and User Group Sources" on page 51

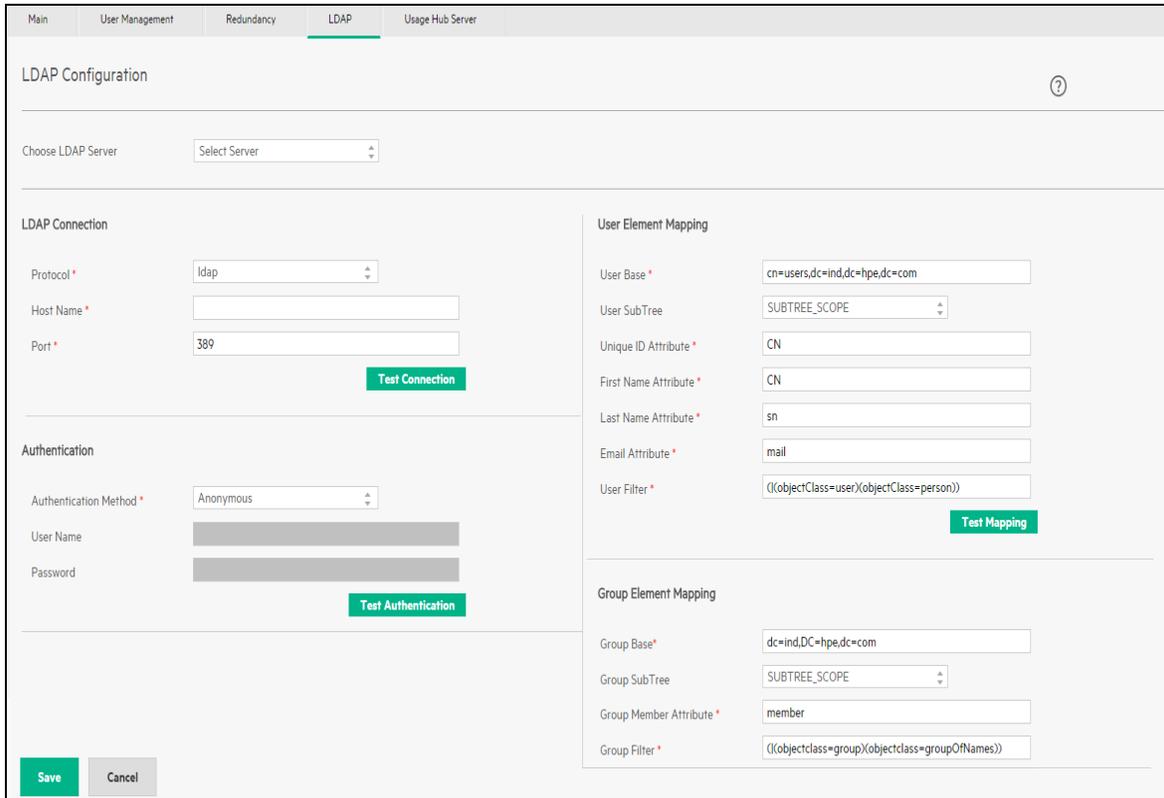
User interface elements are described below:

UI Element	Description
Configure password settings	Enables you to set the options for user password expiration. There are two possible settings: <ul style="list-style-type: none"> • User password will never expire. • User password will expire as per below settings
Reset password on the	Requires each AutoPass License Server user to reset the user's

UI Element	Description
<p>first login for all users</p>	<p>password when they first log in to the AutoPass License Server (<i>default</i>).</p> <p>Note: This option is enabled only if you select the User password will expire as per below settings option.</p>
<p>Change password after <> days</p>	<p>Requires each AutoPass License Server user to change the password after the defined number of days.</p> <p>Note: This option is enabled only if you select the User password will expire as per below settings option.</p>
<p>Enable Email notification while adding or removing users from group</p>	<p>Sends a notification e-mail message to a user when the user is added or removed from a user group. The e-mail message is sent to the address specified for the user in the Users tab (User Management pane). For details, see "Users Tab (User Management Pane)" on page 57.</p>
<p>Configure sources for users and groups</p>	<p>Enables you to select the source for creating AutoPass License Server users and groups.</p> <p>You must select either the AutoPass License Server internal database (DB) or an LDAP server as a source for both users and user groups.</p> <p>Note: The source for users does not have to be the same as the source for the user groups.</p>

LDAP Tab (Configuration Pane)

This tab enables you to define connection options for your LDAP server connection.



To access	Configuration pane > LDAP tab
Important information	<ul style="list-style-type: none"> • After configuring LDAP in the redundancy mode, it is mandatory to restart server where LDAP is configured. • You cant reset the password of default user(admin), in License Server if User Management is set to LDAP Configuration.
Relevant tasks	"Import groups from an LDAP server" on page 55
See also	"User and User Group Sources" on page 51

User interface elements are described below:

UI Element	Description
Choose LDAP server	Enables you to select the type of LDAP server you are using: <ul style="list-style-type: none"> • Enterprise LDAP Server

UI Element	Description
	<ul style="list-style-type: none"> • Microsoft Active Directory Server <p>When you select either type of server, the default properties are displayed in the pane. However, you can configure any of the properties as needed.</p>
LDAP Connection	<p>Enables you to set the specific connection settings for your server, including:</p> <ul style="list-style-type: none"> • Protocol: ldap or ldaps • Host name: The host address for the server • Port: The entry port for the server <p>Note: All fields are required</p>
Authentication Method	<p>Enables you to set the connection authentication properties, including:</p> <ul style="list-style-type: none"> • Authentication method (<i>required field</i>) <ul style="list-style-type: none"> • anonymous (without authentication parameters) • simple (user name and password authentication) • User name/password: The user name and password required for a simple authentication. <p>Note: The user name and password edit fields are enabled only if you select simple as the method of authentication.</p> <p>Example: User Name = uid=admin,ou=system</p>
User Element Mapping	<p>Enables you to configure how users stored on the LDAP server are mapped to their roles in the AutoPass License Server.</p> <p>You can configure the following settings:</p> <ul style="list-style-type: none"> • User Base: The location in the LDAP directory containing user entries (<i>required field</i>) • User SubTree: The sub-directory location in the LDAP server for users (if they are not contained the main directory) <ul style="list-style-type: none"> • OBJECT_SCOPE - Searches in the current object only • ONELEVEL_SCOPE - Searches in the current and one object below • SUBTREE_SCOPE - Searches in the sub tree • Unique ID Attribute: The attribute of the object class that provides the name of the user specified in the object class (<i>required field</i>)

UI Element	Description
	<ul style="list-style-type: none"> • First Name Attribute: The attribute of the object class the provides the first name of the user specified in the object class (required field) • Last Name Attribute: The attribute of the object class the provides the last name of the user specified in the object class (required field) • Email Attribute: The attribute of the object class that provides the email address of the user specified in the object class (required field) • User Filter: The filter that identifies the user entries (required field) <p>Example:</p> <pre>((objectClass=person)(objectClass=applicationProcess))</pre>
<p>User Group Mapping</p>	<p>Enables you to configure how user groups stored on the LDAP server are mapped to their roles in the AutoPass License Server.</p> <p>You can configure the following settings:</p> <ul style="list-style-type: none"> • Group Base: The location in the LDAP server directory containing the user groups (required field) • Group SubTree: The sub-directory location in the LDAP server for user groups (if they are not contained the main directory) • Group Member Attribute: The attribute of the object class the provides the name of the user group specified in the object class (required field) • Group Filter: The filter that identifies the user group entries <p>Example:</p> <pre>(objectClass=groupOfNames)</pre>

AutoPass License Server User and User Group Management - Frequently Asked Questions

Does a AutoPass License Server user have to belong to a user group?

No. However, AutoPass License Server users that are not assigned to user groups are limited to *View-Only* access privileges.

How do I stop a user from logging in to the AutoPass License Server?

In the Users tab (User Management Pane), change the user's status to *inactive*. This blocks the user from logging in to the AutoPass License Server.

How can a user recover a forgotten password?

A user can reset a password in one of the following ways:

- Request that the AutoPass License Server administrator reset the user's password by clicking the **Reset Password** link in the [Users Tab \(User Management Pane\)](#)
- In the Users tab (User Management Pane), use the **Reset Password** link to reset the user's password. For details, see ["Reset a user's password" on page 54](#).

Why do I need to create user groups?

User groups are created to manage products and assign access privileges to users. After creating user groups, AutoPass License Server users are assigned to the groups and access privileges are assigned to the user group by a AutoPass License Server administrator.

Can an administrator assign a privilege level directory to a user?

No. Privileges are assigned by the user group. You must assign or change the access privilege level of the group to which the user belongs.

Note: Any users not assigned to a user group have *View-Only* access privileges.

Can a AutoPass License Server administrator delete LDAP users or user groups from an LDAP server?

No. You can only remove the imported users and user groups from the AutoPass License Server. Removing them from the AutoPass License Server does not delete them from the host LDAP server.

How do I assign the products to which a Product Admin user has administrative access?

In the Manage User Groups tab (User Groups tab), add associated products for each Product Admin group. For details, see ["Associate products with a Product Admin group" on page 56](#).

AutoPass License Server User and User Group Management - Troubleshooting and Limitations

Why are there no options to configure the password settings or email notifications in the User Management tab (Configuration Pane)?

If you selected LDAP as the source for users or user groups, password settings and email notifications are not available for configuration.

Chapter 9: License Management

This chapter includes:

Concepts

- ["Installing Licenses" on the next page](#)
- ["License Usage Reports" on the next page](#)
- ["Searching License Check In and History" on page 72](#)
- ["Archiving and Restoring Licenses" on page 73](#)
- ["Borrowing Licenses" on page 73](#)
- ["License Clean Up" on page 74](#)

Tasks

- ["How to Manage Licenses" on page 74](#)

Reference

- ["License Usage Pane" on page 79](#)
- ["Feature Report Page \(License Usage Pane\)" on page 80](#)
- ["Search Criteria Page \(License Usage Pane\)" on page 86](#)
- ["Search Results Page \(License Usage Pane\)" on page 87](#)
- ["Install License Tab \(License Management Pane\)" on page 89](#)
- ["License Management Tab \(License Management Pane\)" on page 90](#)
- ["Archive License Tab \(License Management Pane\)" on page 91](#)
- ["Borrow License Tab \(License Management Pane\)" on page 92](#)
- ["Borrow License Request Window \(Borrow License Tab\)" on page 94](#)
- ["License Clean Up Tab \(License Management Pane\)" on page 95](#)
- ["**License Management - Frequently Asked Questions" on page 96**](#)
- ["**License Management - Troubleshooting and Limitations" on page 99**](#)

Concepts

Installing Licenses

After installing and configuring the AutoPass License Server, you must install licenses in the AutoPass License Server. This step makes the licenses available for check out operations, and enables you to perform other license management tasks such as reserving licenses for user pools checking out commuter licenses.

You can install licenses by loading a single license key file or multiple license key files.

Note: The size of the license key file cannot be larger than 4 MB.

You obtain license keys on a per-product and per-feature basis. For details on obtaining license keys, see the individual product documentation.

For details on how to install license keys, see ["Install a license" on page 75](#).

License Usage Reports

After installing licenses, the AutoPass License Server provides multiple pages in which you can track and view the licenses currently installed and used on your AutoPass License Server.

The **License Management** tab (License Management pane) displays the basic details about installed feature licenses, including:

- All feature licenses available per product, including their identification number and details
- The installed capacity
- The license start date
- The license expiration date
- The license installation date
- The name of the AutoPass License Server user that installed the licenses and the IP address.

You can export the license report details to Excel. For details on the License Management tab, see ["License Management Tab \(License Management Pane\)" on page 90](#).

In addition, usage details about installed licenses are displayed in the **License Usage** pane. This pane displays additional information about the list of all installed license details, including:

- The feature license identification information, including number and description
- The available license capacity
- The capacity currently checked out as live and commuter licenses

Like the License Management tab, you can export the license report details to Excel. For details, see ["License Usage Pane" on page 79](#).

To view the details of a specific feature license, click the feature name in the License Usage pane to display the **Feature Report** page.

The Feature Report page displays specific check out information about a feature license including:

- Graphs of overall usage, check out type distribution and pool wise usage of a feature and its history.
- The check out start and expiration date
- The type of check out distribution: **Live** or **Commuter**
- The capacity checked out
- Check out and check in details for the license
- The pools to which users who have licenses checked out belong. You can select the required pool.

If a license has the ability to control commuter license properties, you also set the commuter license properties in the Feature Report page.

For details on the Feature Report page, see "[Feature Report Page \(License Usage Pane\)](#)" on page 80.

Searching License Check In and History

From the License Usage pane, you can search through the check in and check out histories of all installed licenses.

You can search based on a number of criteria:

- The feature ID and feature ID version
- The feature description
- The client user attributes for a license with check out and check in history
- The license start and expiration dates

You can then use the search results to purge the server operations history or revoke a license check out.

Purging¹ a license deletes the check in history from the AutoPass License Server. After you purge the history, it is removed from the AutoPass License Server.

Revoking² a license (by an administrator) forcibly checks in a live concurrent license to the AutoPass License Server. If you need a license for a higher priority client user or need to return a borrowed license to another AutoPass License Server, an administrator can revoke a license.

If a connection exists between the AutoPass License Server and the client computer, when a license is revoked, a message is sent to the client user with the checked out license within two minutes and the license is automatically checked into the AutoPass License Server within two minutes. If there is no connection, the AutoPass License Server continues to send the message until the client computer connects with the AutoPass License Server. You cannot revoke the license until the client user connects with the AutoPass License Server (provided the license is still within the expiration period).

Note: Commuter licenses cannot be revoked.

Examples

¹The process of removing the checkin history from the License Server.

²The process of forcibly checking in a live concurrent license to be used for other License Server functions.

Use Case 1

You have an installed capacity of 100 for *FeatureA*. *User1* has a live concurrent license capacity of 40 checked out. If *User2* needs a capacity of 80 for check out, you can search for *User1* using the search results and revoke *User1*'s license.

Use Case 2

You are planning how users will use the available capacity for a product in the next iteration. Using the search criteria described on [Search Criteria Page \(License Usage Pane\)](#), you can search for licenses with an upcoming expiration date so you can see how many licenses will be available on certain dates.

Archiving and Restoring Licenses

If you do not want a specific license to be available for checkout, but you do want to keep it on the AutoPass License Server, you can archive a license.

You can **archive**¹ any unused license that is displayed in the License Management tab. This removes them from the list of currently active licenses (displayed in the License Management tab).

Once a license is archived, you can also delete it from the AutoPass License Server. If you need to restore a license to active use, you can restore the license and it again becomes available for check out operations.

Borrowing Licenses

If a AutoPass License Server needs additional licenses to fulfill client user requests for a product or feature, the AutoPass License Server can **borrow**² them from other AutoPass License Servers.

Borrowed licenses are borrowed temporarily, as you set an expiration date for the license borrowing request. After the expiration period, the license is returned to the AutoPass License Server from which it was borrowed.

You can configure your AutoPass License Server to borrow only from a specific AutoPass License Server or to search the subnet for other available AutoPass License Servers.

Example

FeatureA has an installed capacity of 40. Two users already have licenses for *FeatureA* with the capacity of 15 checked out. If additional users will need license capacity for check out, you can use the borrow option to take the necessary license capacity from another AutoPass License Server.

¹The process of removing a license from active use for check out.

²The process of taking license capacity from another License Server.

License Clean Up

In certain circumstances, the license capacity of selected licenses will be deleted, such as in the following scenarios:

- When commuter licenses are lost due to a client user's system crash
- When a product is configured to detect clock tampering and the system is back dated or clock-tampered

In this case, you can perform [license cleanup](#)¹ to restore the lost capacity.

To perform License Clean Up, you must contact the support team for a License Clean Up key. When you apply the license cleanup key, the license capacity is restored to its previous levels.

Note: Each type of feature or product license has a specific limit for license restoration via license cleanup. For details on viewing and setting the license clean up limits, see the individual product documentation.

Tasks

How to Manage Licenses

This task describes the procedures necessary to manage the licenses installed on your AutoPass License Server.

This task includes the following steps:

- ["Install a license" on the next page](#)
- ["Archive a license" on the next page](#)
- ["Restore an archived license" on the next page](#)
- ["Borrow a license " on page 76](#)
- ["Restore license capacity with License Clean Up" on page 77](#)
- ["Search license check in and check out history" on page 77](#)
- ["Purge the license check in history" on page 77](#)
- ["Revoke a checked out license" on page 77](#)
- ["Manage commuter settings for a feature license" on page 77](#)
- ["Delete a license from the AutoPass License Server" on page 78](#)

¹The process of restoring license capacity for a feature or product due to system crash or clock tampering.

Install a license

1. In the Install License tab (License Management pane), enter the license keys for your products. For details on obtaining license keys, see the individual product documentation.

Note: If you received a license key in the form of a file (such as a .dat file), you can browse to the license file by selecting **Browse Licenses File** and browsing to the directory containing the file. The license file size cannot exceed 4 MB.

2. Click **Next**.
3. In the Install Licenses page, select the licenses to install, and click **Install Licenses**.

The licenses are installed on the AutoPass License Server and are displayed in the License Management tab (License Management pane).

Note: License key installed can be locked to a lock value. This lock value is displayed in the **Install Licenses** page.

Refer to individual product documentation to validate if such licenses are supported by the product.

If a license locked to the specified lock value is installed, any licenses locked to IP address (of the same feature ID) of APLS is auto archived. Two different feature licenses, one locked to IP and another locked to lock value specified can coexist.

Archive a license

1. In the License Management tab (License Management pane), select the unused licenses you want to archive.
2. Click **Archive**.

The licenses are removed from the list of installed licenses in the License Management tab and are unavailable for check out operations. A list of all archived licenses is displayed in the Archived License tab (License Management pane).

Restore an archived license

1. In the Archived License tab (License Management pane), select the product whose archived licenses you want to restore.
2. Select the features to restore.
3. Click **Restore**.

The licenses are again displayed in the License Management pane and client users can check them out.

Note: If a IP locked licenses are auto archived, it cannot be restored unless all the licenses locked to a lock value belonging to same feature are either deleted or archived.

Borrow a license

1. In the Borrow License tab (License Management pane), select the Product for which you want to borrow a license.
2. Click **Borrow License**.
3. On the Borrow License page, enter the following details:
 - Select the Product for which you want to borrow a license.
 - The feature ID and version for which you want to borrow a license
 - The license capacity to borrow
 - The expiration date for the borrowed license
 - The server information. You can enter the server information in the following ways:
 - Select **Configure License Server** and provide the **Host Name** or **IP**, the **Port**, and **Protocol** of another AutoPass License Server
 - Select **Discover AutoPass License Server** and browse through the subnet for an available AutoPass License Server

3. Click **Borrow**.

The borrowed license capacity is displayed in the Manage Borrowed Licenses window (Borrow License tab) and is added to the license capacity listed in the License Management tab.

Return a borrowed license

1. In the Borrow License tab (License Management tab), select the product for which you need to return licenses.
2. Select the license to return.
3. Click **Return**.

The license is returned to the AutoPass License Server from which the license was borrowed and the borrowed capacity is removed from the list of borrowed licenses in the Borrow License tab and is removed from the License Management tab.

Clear the borrowing history

1. In the Borrow License tab (License Management pane), select the product for which you want to view the borrowing history. The Borrowed License list and the Checked-In History list for that product are displayed.
2. In the Checked-In History list, select the check box for the history to delete.
3. Click **Delete**.

A message confirming the history deletion is displayed at the top of the window and the selected history items are no longer displayed in the borrowing history.

Restore license capacity with License Clean Up

1. In the License Clean Up tab (License Management pane), enter the license cleanup key you received from the support team and click **Submit**.
2. In the Clean Up Window, select one or more license checkouts to clean up and click **Clean Up**.

Note: Each license has a limit to the capacity possible for license cleanup. For details on setting limits to license cleanup, see the individual product documentation.

Search license check in and check out history

1. In the License Usage pane, click Search .
2. In the Search window, enter the search criteria.
3. Click **Search**.

All installed licenses that match your search criteria are displayed in the Search Results window.

Purge the license check in history

After the search results are displayed in the Search Results page, click **Purge**.

The history is removed from the AutoPass License Server.

Revoke a checked out license

1. After performing a search, in the Search Results window (License Usage pane), select the license that you need to revoke.
2. Click **Revoke** and confirm the revocation.

The license is returned to the AutoPass License Server.

Manage commuter settings for a feature license

1. In the License Usage pane, click the checkbox for the feature for which you want to manage commuter license settings, and click **Manage Commuter**. A message informing you of the successful enablement of commuter license settings is displayed. Click **OK**.
2. The Feature Report page for that feature opens.

Note: Not all features are enabled for modifying commuter check out settings. Only those features with a cleared and enabled check box can be modified.

2. In the Commuter Checkout Settings area, click **Edit**.
3. Enter the maximum number of days allowed and the maximum capacity allowed for a commuter license check out.
4. Click **Save Changes**.

The changes are displayed under the Commuter Checkout Settings for the feature.

Note: You must have administrator access privilege permissions to modify the commuter check out settings.

Delete a license from the AutoPass License Server

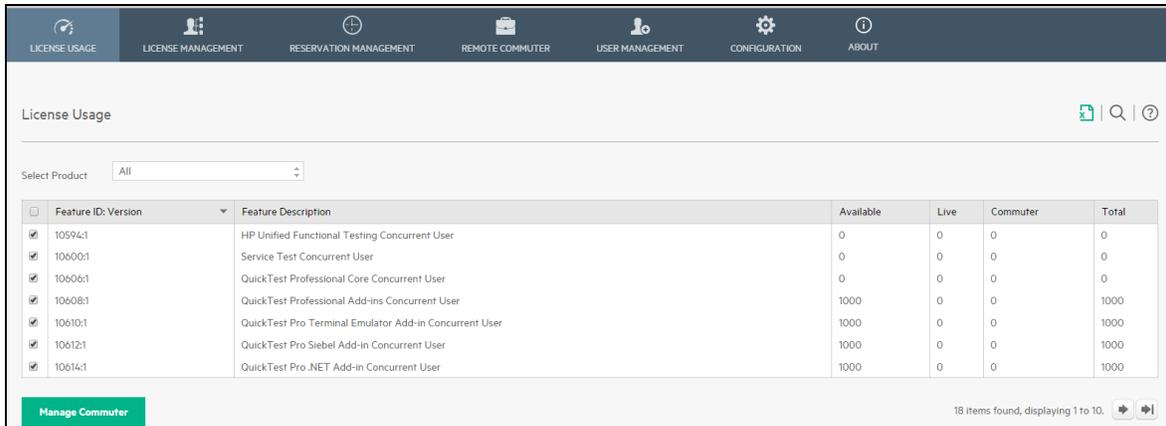
1. In the Archived License tab (License Management pane), select the product for which you want to delete licenses.
2. Select the feature you want to delete.
3. Click **Delete** and confirm the deletion.

The license is removed from the AutoPass License Server.

Reference

License Usage Pane

This pane enables you to view the installed licenses and license capacities.



To access	Select the License Usage node in the AutoPass License Server menu bar.
Important information	<ul style="list-style-type: none"> The licenses displayed in this pane are the same as the licenses displayed in the License Management tab (License Management pane). For details, see "License Management Tab (License Management Pane)" on page 90. If a feature is automatically enabled for commuter check out, the feature check box is displayed as a selected, disabled check box. If a feature is automatically disabled for commuter check out, the feature check box is displayed as a cleared, disabled check box. If a feature is available to have its commuter license check out settings modified, it is displayed in this pane as a cleared, enabled check box.
Relevant tasks	"How to Manage Licenses" on page 74
See also	"License Usage Reports" on page 71

User interface elements are described below:

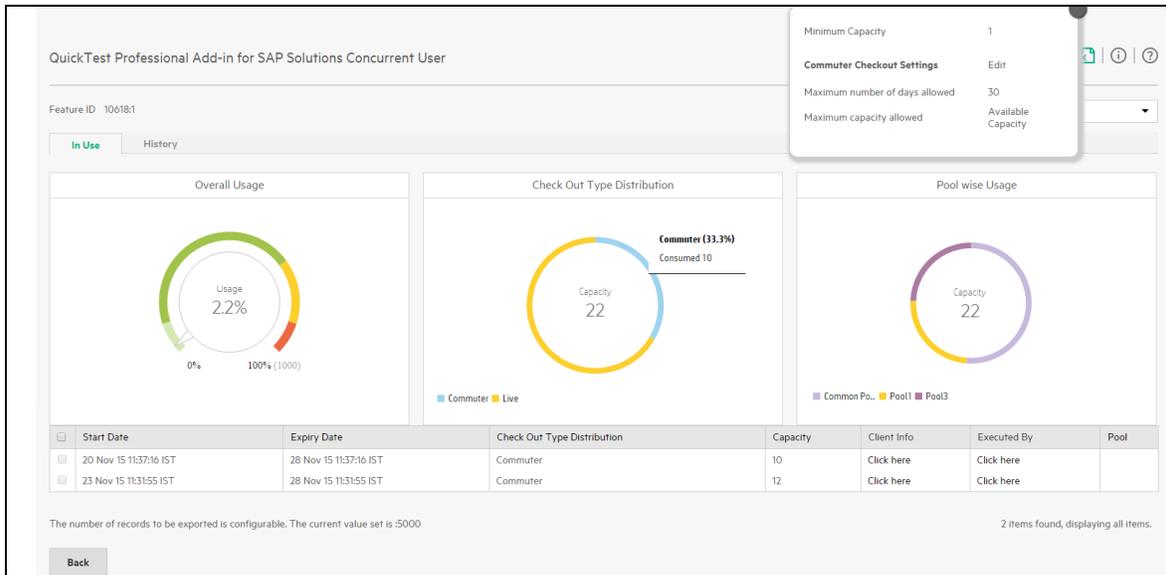
UI Element	Description
Feature ID: Version	The specific feature number and version for each feature of the selected product in the drop-down.
Feature Description	A textual description of a feature.

UI Element	Description
Available	The license capacity currently available for client user check out.
Live	The license capacity currently checked out as live, concurrent licenses.
Commuter	The license capacity currently checked out as commuter licenses.
Total	The total installed license capacity.
	Export to Excel. Exports the currently displayed License Usage report to an Excel file.
Manage Commuter	Enables you to modify the commuter check out settings for a feature, if enabled.
	Opens the Search window, enabling you to search the check out and check in history. For details, see " Searching License Check In and History " on page 72 and " Search Criteria Page (License Usage Pane) " on page 86.

Feature Report Page (License Usage Pane)

This page enables you to view the license check out report and details for a specific feature.

In Use



To access	In the License Usage pane, click the Feature ID: Version link for a specific feature.
Important information	The Commuter Checkout Settings area is editable only if the feature allows modifying commuter check out settings and you enabled editing of the settings by clicking Manage Commuter for the selected feature in the License Usage pane.
Relevant tasks	"How to Manage Licenses" on page 74
See also	"License Usage Reports" on page 71

UI Element	Description
Feature ID: Version	The feature number and version.
In Use tab	<p>The graphs of overall usage, check out type distribution and pool wise usage of a feature.</p> <ul style="list-style-type: none"> Overall Usage - The graph shows the percentage of usage and is differentiated as below <ul style="list-style-type: none"> From 0% to 10% - Minimal usage From 10% to 70% - Optimal usage From 70% to 90% - Heavy usage From 90% to 100% - Maximum usage Check Out Type Distribution - The check out type i.e Live and Commuter is denoted and tool tip provides check out type percentage

UI Element	Description
	<p>and consumed capacity.</p> <ul style="list-style-type: none"> • Pool Wise Usage - The pool wise usage graph denotes total capacity and pool distribution. Also provides the tool tip which denotes the consumed and reserved capacity. <div style="background-color: #f0f0f0; padding: 5px;"> <p>Note:</p> <ul style="list-style-type: none"> • The pool wise usage graph is displayed when individual pool is not selected. When a single pool is selected the Total Capacity and Reserved Capacity for Pool is displayed. • If the reservation capacity was changed after check out when a particular pool is selected if the checked out capacity is more than the reserved capacity, the usage graph shows more than 100%. </div>
	<p>Export to Excel. Exports the currently displayed report to Excel. The maximum number of records which can exported is 5000.</p>
	<p>The information of minimum capacity, commuter checkout settings, maximum number of days allowed and maximum capacity allowed.</p> <ul style="list-style-type: none"> • Minimum Capacity - The minimum capacity a client user can check out in a checkout request. • Commuter Checkout Settings - Enables you to select settings for commuter check out of the feature license, including: <ul style="list-style-type: none"> • Maximum number of days allowed - This number is limited by the type of license mentioned in the Product Description for a feature. • Maximum capacity allowed - The default setting is Available Capacity, which checks out all available capacity as part of a commuter check out. Change this number if you want to limit the capacity for each check out.
Select Pool	Enables you to select the required pool from the drop down.
Start Date	The start date of a license check out.
Expiry Date	The expiration date of a license check out.
Check Out Type Distribution	The type of check out: Live (concurrent license) or Commuter .
Capacity	The capacity checked out by a client user.
Client Info	The user attributes of the user who has checked out the license. Click the Click here link to view the details.
Executed By	The user that checked out the license. Click the Click here link to view the details.
Pool	The user pool to which the client user who has checked out a license

UI Element	Description												
	<p>belongs.</p> <p>Note: Even if a single license is checked out from a particular pool this field displays the same pool details rather than showing the shared pool details.</p> <p>Example:</p> <p>In this scenario there are two pools and the available capacity is 100, as detailed below:</p> <table border="1" data-bbox="493 619 1300 848"> <thead> <tr> <th>Pool Name</th> <th>Capacity</th> <th>Total Capacity</th> </tr> </thead> <tbody> <tr> <td>Pool 1</td> <td>10</td> <td>100</td> </tr> <tr> <td>Pool 2</td> <td>10</td> <td></td> </tr> <tr> <td>Shared</td> <td>80</td> <td></td> </tr> </tbody> </table> <p>Use Case 1 : A client user makes a check out request for capacity of 9. This request is fulfilled using Pool 1.</p> <p>Use Case 2: A client user makes a check out request for capacity of 9. This request is fulfilled using Pool 2.</p> <p>Use Case 3: A client user tries to check out request for capacity of 10. This request is fulfilled using 1 capacity from Pool 1 and 8 capacity from shared pool.</p> <p>The pool details in the table in the In Use and History tab displays Pool 1 details itself as 1 capacity is checked out from Pool 1.</p>	Pool Name	Capacity	Total Capacity	Pool 1	10	100	Pool 2	10		Shared	80	
Pool Name	Capacity	Total Capacity											
Pool 1	10	100											
Pool 2	10												
Shared	80												

History

|

To access	In the License Usage pane, click the Feature ID: Version link for a specific feature and navigate to History tab.
Important information	<p>The Commuter Checkout Settings area is editable only if the feature allows modifying commuter check out settings and you enabled editing of the settings by clicking Manage Commuter for the selected feature in the License Usage pane.</p> <p>When a license is checked out and checked in for a particular feature the usage data is reflected in the In Use and History page respectively post each action and in case of inactivity, any usage data is refreshed every eight hours.</p> <p>The data in the History tab will be shown only from the day the AutoPass License Server is upgraded.</p>

Relevant tasks	"How to Manage Licenses" on page 74
See also	"License Usage Reports" on page 71

User interface elements are described below:

UI Element	Description
Feature ID: Version	The feature number and version.
History tab	<p>The graphical representation of check out and check in history is displayed.</p> <p>The pool wise differentiation is denoted and also the tool tip with</p> <ul style="list-style-type: none"> • The name of the pool • Pool wise usage maximum consumed and • The number of users. <p>You can select required options with the help of the radio buttons available below the graph.</p> <ul style="list-style-type: none"> • Maximum - The graph displays only the maximum check outs at any point of time in the selected date range. • Average - The graph displays sum of all the checkouts divided by number of checkouts in the selected date range. <p>The feature wise checked in and checked out history details in numbers at any given point of time i.e</p> <ul style="list-style-type: none"> • Maximum • Average <p>The horizontal red line indicates the current total license installed at the feature level. If a pool is selected, it represents the capacity reserved for a particular pool.</p>
Date Range	Enables you to select the range with the options today, yesterday, last 7 days, last 30 days, this month, last month and custom date.
Select Pool	Enables you to select the required pool from the drop down.
Start Date	The start date of a license check out.
Expiry Date	The expiration date of a license check out.
Check Out Type Distribution	The type of check out: Live (concurrent license) or Commuter.
Capacity	The capacity checked out by a client user.
Client Info	The user attributes of the user who has checked out the license. Click the Click here link to view the details.

UI Element	Description
Executed By	The user that checked out the license. Click the Click here link to view the details.
CheckIn Time	The check in time of a license
Pool	The user pool to which the client user who has checked out a license belongs. Refer to " Even if a single license is checked out from a particular pool this field displays the same pool details rather than showing the shared pool details. " on page 83 for more details.

Search Criteria Page (License Usage Pane)

This page enables you to determine the criteria for searching installed licenses.

Search ?

Select Product

Feature ID

Feature ID: Version

Feature Description

IP Address

Host Name

User Name

Client ID

Start Date

Expiry Date

To access	In the License Usage pane, click the Search button  .
Important information	The searchable options for the IP Address , Host Name , User Name , and Client ID should be the same as the user pool attributes listed in the Pool Management tab (Reservation Management tab).
Relevant tasks	"Search license check in and check out history" on page 77

See also	<ul style="list-style-type: none"> • "License Usage Pane" on page 79 • "Search Results Page (License Usage Pane)" below • "Searching License Check In and History" on page 72 • "Pool User List Section (Pool Management Tab)" on page 113 • "Client User Attributes" on page 103
-----------------	--

User interface elements are described below:

UI Element	Description
Feature ID	The number of the feature.
Feature ID: Version	The version number of the feature (without the feature ID).
Feature Description	The textual description of the feature. You can use this field if you are unable to remember the specific feature number.
IP Address	The IP address of a client user that has checked out a license.
Host Name	The host address of the client user that has checked out a license.
User Name	The user name for the client user that has checked out a license.
Client ID	The computer ID for the client user that has checked out a license.
Start Date	The start date of a license check out.
Expiry Date	The expiration date of a license check out.

Search Results Page (License Usage Pane)

This page displays the applicable licenses according to your search criteria.

Feature Description	Start Date	Expiry Date	Check Out Type Distribution	Capacity	Client Info	Executed By	Product	Pool
QuickTest Professional Add-in for SAP Solutions Concurrent User	20 Nov 15 11:37:16 IST	28 Nov 15 11:37:16 IST	Commuter	10	Click here	Click here	HP UFT_1250	
QuickTest Professional Add-in for SAP Solutions Concurrent User	23 Nov 15 11:31:55 IST	28 Nov 15 11:31:55 IST	Commuter	12	Click here	Click here	HP UFT_1250	
QuickTest Professional Add-in for SAP Solutions Concurrent User	19 Nov 15 14:55:00 IST	19 Nov 15 15:05:00 IST	Live	1	Click here	Click here	HP UFT_1250	

3 items found, displaying all items.

[Purge](#) [Back](#) Email This Report : [Send Mail](#)

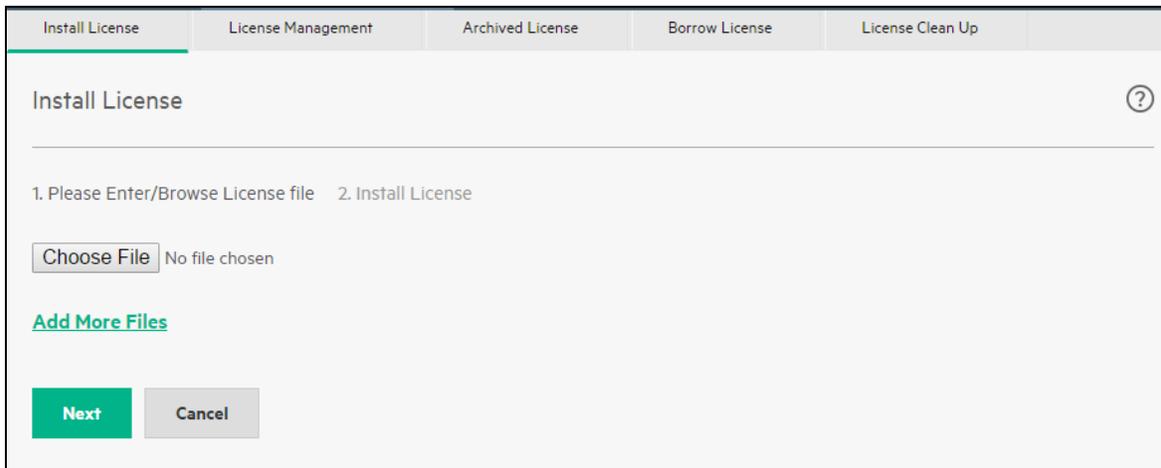
To access	Click Search in the Search window after defining search parameters.
Relevant tasks	<ul style="list-style-type: none"> • "Search license check in and check out history" on page 77 • "Purge the license check in history" on page 77 • "Revoke a checked out license" on page 77
See also	<ul style="list-style-type: none"> • "Search Criteria Page (License Usage Pane)" on the previous page • "Searching License Check In and History" on page 72

User interface elements are described below:

UI Element	Description
Feature Description	The textual description of the licenses returned from the search results.
Start Date	The start date of the license check out.
Expiry Date	The expiration date of the license check out.
Check Out Type Distribution	The type of license check out: Live or Commuter .
Capacity	The capacity checked out for the license.
Client Info	The client user that checked out the license. Click Click here to display the client user attributes for the check out.
Executed By	The user that performed the check in and check out operation. Click Click here to display the details for the check out.
Product	The product to which the product belongs.
Pool	The user pool to which the client user that performed the check out belongs.
	Export to Excel. Exports the currently displayed report to Excel.
Purge	Deletes the histories from the AutoPass License Server.
Revoke	Automatically checks the selected license into the AutoPass License Server.

Install License Tab (License Management Pane)

This tab enables you to install licenses for your products.



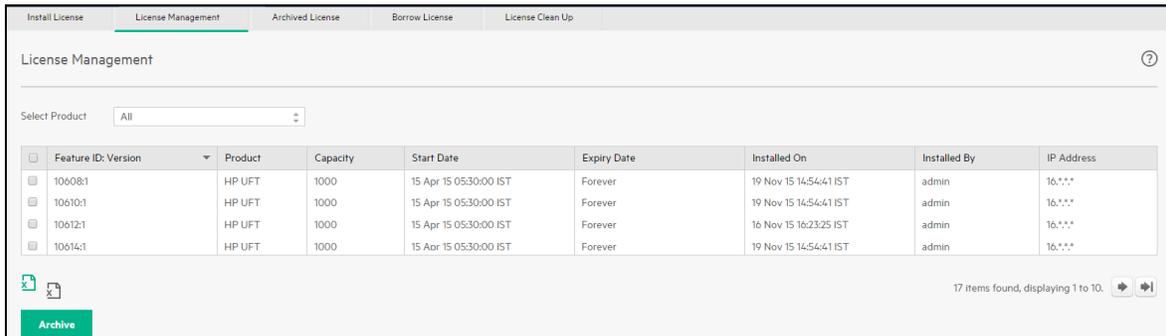
To access	License Management pane > Install License tab
Important information	License key files cannot exceed 4 MB.
Relevant tasks	"Install a license" on page 75
See also	"Installing Licenses" on page 71

User interface elements are described below:

UI Element	Description
Enter license keys	Enables you to enter a single license key or group of license keys for installation.
Browse Licenses File	Enables you browse and upload a license key file containing license keys to be installed.

License Management Tab (License Management Pane)

This tab displays the information about all installed licenses and enables you to archive licenses.



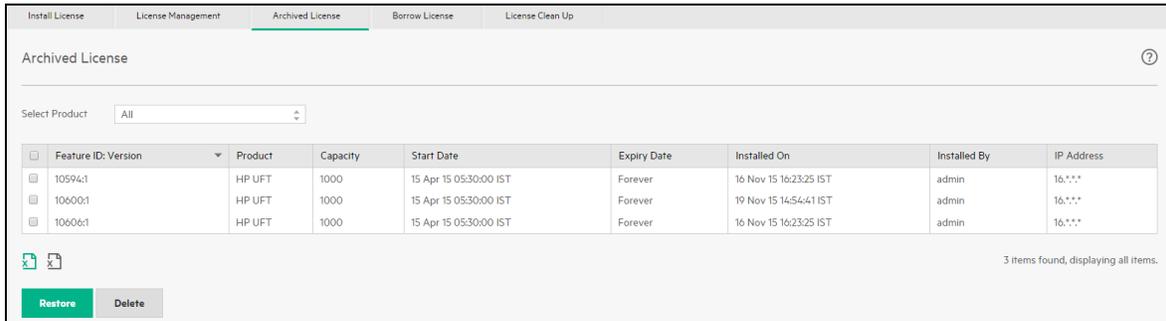
To access	License Management Pane > License Management tab
Relevant tasks	"How to Manage Licenses" on page 74
See also	"Archiving and Restoring Licenses" on page 73

User interface elements are described below:

UI Element	Description
Feature ID: Version	The number for the feature and its version number.
Product	The product to which a feature belongs.
Capacity	The total installed capacity for each installed license.
Start Date	The starting date of the installed license.
Expiry Date	The expiration date of the installed license.
Installed On	The installation date of the installed license.
Installed By	The name of the AutoPass License Server user that installed the licenses.
IP Address	The IP address of the user installing the licenses.
	Export to Excel. Exports the currently displayed report to Excel.
	Export Raw License to Excel. Exports the license keys for the currently displayed licenses to Excel.
Archive	Archives the selected license.

Archive License Tab (License Management Pane)

This tab displays the list of all archived licenses enables you to restore archived licenses to active use or delete them permanently.

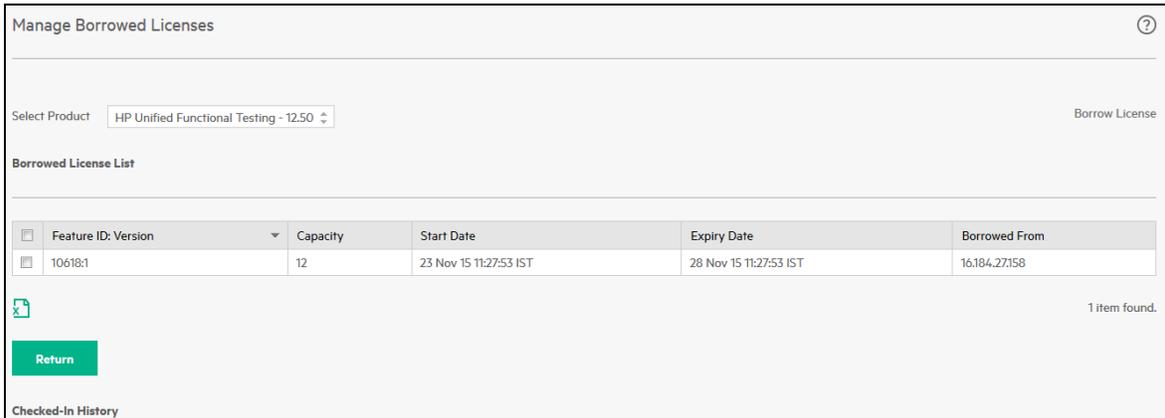


To access	License Management pane > Archived Licenses tab
Important information	Licenses cannot be restored if they are expired.
Relevant tasks	"Restore an archived license" on page 75
See also	"Archiving and Restoring Licenses" on page 73

The user interface elements are the same as those displayed in the License Management tab. For details, see ["License Management Tab \(License Management Pane\)" on the previous page.](#)

Borrow License Tab (License Management Pane)

This tab displays all borrowed licenses and borrowing history, and enables you to borrow licenses from other AutoPass License Servers.



To access	License Management pane > Borrow License tab
Relevant tasks	<ul style="list-style-type: none"> • "Borrow a license " on page 76 • "Return a borrowed license" on page 76 • "Clear the borrowing history" on page 76
See also	<ul style="list-style-type: none"> • "Borrowing Licenses" on page 73 • "Borrow License Request Window (Borrow License Tab)" on page 94

User interface elements are described below:

UI Element	Description
Feature ID: Version	The feature number and version.
Capacity	The capacity borrowed for the selected feature from another AutoPass License Server.
Start Date	The date on which the license borrowed begins.
Expiry Date	The date on which the license borrowed expires.
Borrowed From	The AutoPass License Server from which you borrowed a license.
	Export to Excel. Exports the currently displayed report (from the Borrowed License List or the Checked-In History List) to Excel.
Borrow License	Opens the Borrow License window, enabling you to find a AutoPass License

UI Element	Description
	Server from which to borrow a license. For details, see " Borrow License Request Window (Borrow License Tab) " on the next page.

Borrow License Request Window (Borrow License Tab)

This window enables you to borrow licenses from other AutoPass License Servers.

To access	In the Borrow License tab, click the Borrow License link.
Relevant tasks	"Borrow a license " on page 76
See also	<ul style="list-style-type: none"> • "Borrowing Licenses" on page 73 • "Borrow License Tab (License Management Pane)" on page 92

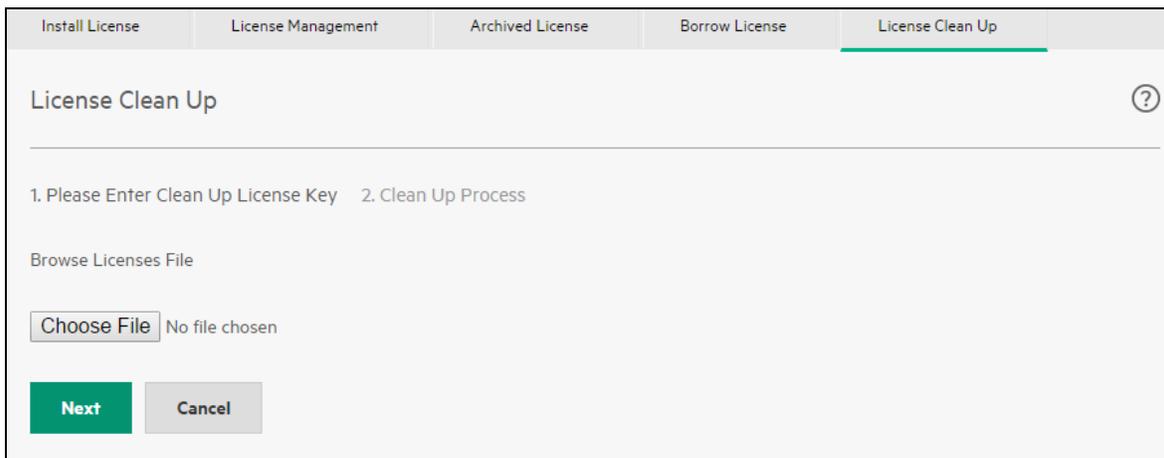
User interface elements are described below:

UI Element	Description
Select Product	The product for which you want to borrow licenses.
Feature ID: Version	The feature for which you want to borrow licenses.
Capacity	The capacity that you want to borrow.
Expiry Date	The date on which the borrowing request ends.
Configure License Server	<p>Enables you to enter the details for a specific AutoPass License Server from which to borrow the licenses.</p> <p>To configure the connection, enter the following:</p> <ul style="list-style-type: none"> • The Host Name or IP for the lending server • The Port for the lending server • The connection protocol: HTTP or HTTPS

UI Element	Description
Discover License Server	Enables you to select other AutoPass License Servers on the same subnet. Select a AutoPass License Server from the list. Click Discover Again to refresh the list.
Borrow	Completes the borrowing request.
Manage Borrowed Licenses	Returns to the Managed Borrowed Licenses window, which displays the list of borrowed licenses and check in history.

License Clean Up Tab (License Management Pane)

This tab enables you to restore lost license capacity by performing license cleanup.



To access	License Management pane > License Clean Up tab
Important information	You must have a license Clean Up key to perform license cleanup. Contact customer support to receive a key.
Relevant tasks	"Restore license capacity with License Clean Up" on page 77
See also	"License Clean Up" on page 74

User interface elements are described below:

UI Element	Description
Please Enter Clean Up License Key	Enter the License Clean Up Key that you received from support.

License Management - Frequently Asked Questions

The following are frequently asked questions about managing licenses in the AutoPass License Server.

Where can I see a report of all users that have a license checked out?

In the License Usage pane, click the **Feature ID: Version** link to open the Feature Report for that feature license. The Feature Report displays the usage information for a selected feature license. For details, see "[Feature Report Page \(License Usage Pane\)](#)" on page 80.

Where can I find a summary of the currently used license capacities for a license?

In the License Usage pane, you can see a report of the **Available** license capacity, the currently checked out **Live** capacity, and the currently checked out **Commuter** license capacity.

Why is there an increase in the total capacity of a feature in the License Usage pane?

The capacity of a feature can increase due to one of the following reasons:

- New licenses are installed.
- The capacity for the feature is borrowed from other AutoPass License Servers.

Why is there a decrease in the total capacity for a feature in the License Usage pane?

The capacity of a feature can decrease due to one of the following reasons:

- Licenses for a feature are archived.
- Licenses for a feature expired.
- Borrowed licenses are returned to the AutoPass License Server from which they were borrowed.

Why is the Pool field blank for some of the licenses listed?

The blank field indicates that the client user that checked out the license does not currently belong to any user pool. For details on user pools, see "[AutoPass License Server Client User Pools](#)" on page 104

How can I purge the license check in history?

License operations history can be purged (deleted permanently) in the following ways:

- Search the records in the Search Page and manually delete them.
- Configure the purge settings in the Main Configuration page. For details, see "[Main Configuration Tab \(Configuration Pane\)](#)" on page 24.

How can an administrator prevent a client user from misusing a license?

An administrator or product administrator can forcibly check in misused licenses by using the **Revoke** option for a license.

How can I reactivate an archived license that is not expired?

Under the Archive License tab (License Management pane), select the licenses to reactivate and click **Reuse**.

Can a client user check licenses into a clock-tampered AutoPass License Server?

Yes.

How to make the Clock Tampered License Keys to work?

AutoPass enable "Clock Tampering" detection for set of features, hence if we install the licenses and tamper with system time, all the features which are enabled for "clock tampering" are blocked.

There are two ways to make the clock tampered license keys to work,

- If you move the system back to the original time from the backdated time, then the all license keys are enabled again.

OR

- In case, if you want to stay in back dated time, then you need to approach HP support to get a "Cleanup License" key. The generation of cleanup key is only through APSC, hence the Product/AutoPass can keep a track of the keys generated. The API to perform clock tampering cleanup is "public virtual String performCleanup(String argLicKey)".

UFT has not enabled clock tampering at client side, so it is mute to create clean up keys for client.

Clock Tampering is detected in my machine and installed licenses have been blocked. if I try installing new Licenses, they are not recognized. Is this expected behavior?

Yes. Existing license keys and newly installed keys are blocked when clock tampering is detected. Remove all the keys backdate the system and reinstall the license keys.

Clock tampering is for the whole list of features for which clock tampering is enabled, irrespective of the time in which he has installed the license key.

How do I recover the license capacity if the system is back-dated and then returned to the correct date?

Restart the AutoPass License Server to recover the license capacity.

Why is the license capacity displayed as zero after the system is back-dated?

The AutoPass License Server is set up in such a way that a feature's capacity is blocked when the system time is back-dated. Perform license cleanup and restart the AutoPass License Server to recover the license capacity.

However, if the system is reset to a future date different than that of a date that was known to the AutoPass License Server, the feature's license capacity is automatically recovered.

How do I permanently delete a license from the AutoPass License Server?

You must archive it before deleting it. Once archived, you click **Delete** in the Archived Licenses tab (License Management pane) and the license is removed from the AutoPass License Server.

If I received a .dat file containing licenses, can I install the licenses on the AutoPass License Server?

Yes. In the Install License tab (License Management pane), select the option for Browse License File. Browse to the directory containing the license file and install the licenses from that file.

Note: License key files cannot be larger than 4 MB.

If I previously archived a license, can I restore it to active use again?

Yes. In the Archive License tab (License Management pane), select the licenses to restore and click **Restore**. The licenses are added to the licenses listed in the License Management tab (License Management pane), and client users can check out license capacity from this license.

In order to borrow a license, do I have to know the details of other AutoPass License Servers?

No. You can click **Discover License Server** in the Borrow License Window (Borrow License tab) and search the subnet for available AutoPass License Servers.

How do I return a borrowed license before the borrowing request expires?

In the Borrow License tab, select the license to return from the Borrowed Licenses list and click **Return**.

Do I have to specify a license capacity to borrow when making a borrowing request?

Yes.

Where do I find the key for license cleanup?

Contact the support team to receive a License Clean Up key.

How to find why capacity is not available in AutoPass License Server?

Below are the reasons the capacity may not be available:

- All the capacity has been checked out by clients. In case the admin wants to release the capacity, then he/she can either revoke or clean up licenses for Live and Commuter respectively.
- If the license is archived in the License Server. Admin can restore the archived license.
- If the system has been clock tampered.

What is NO locking code license?

A license keys which can work with any system is called NO locking code. A license key in UFT has device ID lock type and a wild carded value "any" can be used to generate this type of license. The option of allowing no locking code is dependent on the product.

What is TERM and PERPETUAL license?

- Term license are which licenses keys which will expire within the time limit specified during license key generation.
- Perpetual license are those that do not expire.
- Concurrent license are those licenses which are installed on License Server, this can be either Term or Perpetual.

License Management - Troubleshooting and Limitations

The following are frequently asked questions about problems encountered while managing licenses in the AutoPass License Server.

After installing licenses in the AutoPass License Server, why am I unable to view the license details in the License Usage pane?

The product is not yet configured in the AutoPass License Server. Perform a live check out to configure the product and display the Feature Report for a feature.

Why am I unable to check out licenses?

A client user cannot check out licenses for one of the following reasons:

- The client belongs to a user pool that is blocked. For details, see ["Restricting or Blocking User Pools" on page 107](#).
- The client user belongs to a restricted user pool and the requested capacity is not available for that pool.
- The request capacity is not available for that feature.

Why do I get a message "Lock Type not supported" when installing licenses?

This error message specifies that the installed license keys are locked to a particular IP address range. For example, if the license is locked to IP range 16.*.*.*, it cannot be installed in a AutoPass License Server having an IP address 15.1.1.1.

Why am I unable to archive a license?

You can archive licenses only if all the checked out licenses for that feature are returned.

Why is the **Revoke** option not displayed?

The **Revoke** option is displayed only if there are valid live licenses currently checked out.

After performing license cleanup, not all of my license capacity was restored. Why?

Each product or feature has a specific limit for license cleanup. This limit is configured in the license key file.

Why is the history graph not displayed in the License Report page?

There could be an issue with DB connection to retrieve the usage for the graph. To resolve:

1. Stop the AutoPass License Server service.
 - In windows, run the services.msc. Find “HPE AutoPass License Server” service and stop the service.
 - In Linux, run the command - “service hpLicenseServer stop”
2. Edit the dbconfig.xml file in the APLS data folder and modify the value for <property name="connection.pool_size">20</property> to 30. The default location:
 - In Windows, “C:\ProgramData\HP\HP AutoPass License Server\AutoPass\LicenseServer\data\conf”
 - In Linux, “/var/opt/HP/HP AutoPass License Server/AutoPass/LicenseServer/data/conf”
3. Start the AutoPass License Server service,
 - In windows, Go to run->services.msc. Find “HPE AutoPass License Server” service and start the service.
 - In Linux, use command in the command prompt , “service hpLicenseServer start”

Chapter 10: Client User Management

This chapter includes:

Concepts

- ["License Server Client Users - Overview" on the next page](#)
- ["Client User Attributes" on page 103](#)
- ["AutoPass License Server Client User Pools" on page 104](#)
- ["License Reservation Priority" on page 106](#)
- ["Feature-Based vs. Product Based Reservation" on page 106](#)
- ["Restricting or Blocking User Pools" on page 107](#)

Tasks

- ["How to Manage Client User Access" on page 109](#)

Reference

- ["Pool Management Tab" on page 112](#)
- ["Pool User List Section \(Pool Management Tab\)" on page 113](#)
- ["Pool to Product Mapping List \(Pool Management Tab\)" on page 115](#)
- ["Featured-Based/Product-Based Reservation Tab" on page 116](#)

["Client User Management - Frequently Asked Questions" on page 119](#)

["Client Users Management - Troubleshooting and Limitations" on page 121](#)

Concepts

License Server Client Users - Overview

After configuring the AutoPass License Server for use and installing licenses, you should create a list of client users who are able to access the AutoPass License Server. A **client user**¹ is a local user who accesses the AutoPass License Server via their local software installation.

When a client user starts the local copy of their software, the software's license mechanism sends a request for license check out to the AutoPass License Server. The AutoPass License Server recognizes the user by specific attributes entered and linked with the user's profile. For details, see ["Client User Attributes" on the next page](#).

Depending on the user's details and settings, the AutoPass License Server finds and checks out an appropriate license for the client user. For details on user access to different types of licenses, see ["AutoPass License Server Client User Pools" on page 104](#)

You can choose to give a client user full feature access to a specific software program, or you can limit which features are available for license check out. Furthermore, you can restrict or block a client user's ability to access or check out available licenses. For details, see ["Restricting or Blocking User Pools" on page 107](#)

Example

In *ProductA*, you can choose to load selected environments, such as Web, .NET, Java, Standard Windows, and Oracle. In addition, *ProductA* is sold in conjunction with a defect tracking program (*ProductB*). Thus, you can have licenses that combine *ProductB* and *ProductA* or simply run *ProductA* as a standalone application.

You have a number of licenses for *ProductA* installed on the AutoPass License Server. Some of these licenses enable full access to all features of *ProductA*, where as others are specific to those features specific to the Web, .NET, Java, Standard Windows, and Oracle environments. There are also additional licenses for *ProductA* with access to *ProductB*.

When a client user accesses the License Server, the appropriate license is checked out. Depending on your configuration of the user pools, the AutoPass License Server checks out a license for all *ProductA* features, a specific *ProductA* environment, or the *ProductA/ProductB* common features.

Once the session or license expires on the client user's computer, the license is removed from the client computer and is automatically checked in to the AutoPass License Server. If a license checked out to a client user is expired, the client user cannot check in the license.

¹A local user that accesses the License Server to check in or check out a license for a local program installation.

Client User Attributes

When a client user sends a request to the AutoPass License Server, the user is recognized by the client **user attributes**¹. These attributes confirm the identity of the client trying to access the AutoPass License Server and enable the local program to check in a license.

The AutoPass License Server can identify a client user by multiple attributes:

- **User name:** An identifiable name given to each specific user
- **IP Address:** The IP address of the client user's computer or the common IP address that a group of client users access to connect to the AutoPass License Server
- **Host ID:** The hosting address of a client user's computer or the common host address shared by a group of client users
- **Client ID:** An identification number specific to the client machine

When a client user accesses the AutoPass License Server, the AutoPass License Server checks the client user's information against the client user's attributes saved in the User Management system of the AutoPass License Server. If the client user computer's details match the attributes, the AutoPass License Server checks out a license to the client user making the request. If even one of the client user's details does not match the attributes stored in the AutoPass License Server (even if that attribute was simply not entered originally when the client user was created), the AutoPass License Server can prevent the client user from checking out a license.

It is not necessary to enter all the details for each client user. However, entering all available details for each client user is recommended.

Example

The following attributes are stored for four users:

User Name	IP Address	Host ID	Client ID
User1	192.168.12.54	pool1.host.com	5245rc9e56g648f6
User2	192.168.1.86		4532rac4df15f635
User3	172.31.255.1		
User4	172.20.84.6		

If a client user with the User Name *User 1*, the Host ID *pool2.host.com*, the IP Address *192.168.1.86*, and the Client ID *4532rac4df15f635* then tries to access the License Server, the client's request is denied. Since the Host ID *pool2.host.com* is not included in the attribute list, this client is not able to access the available licenses.

¹The details entered for each user. These details can include the client user's user name, IP address, Host ID, or Client ID.

AutoPass License Server Client User Pools

In order for client users to access and check out licenses, each client user has to be assigned to a **user pool**¹.

You can create user pools to organize and maintain client users in any number of ways: users of a specific feature, users of a specific product, users with common attributes, and so on. Client users can be assigned to multiple user pools.

In addition, membership in any user pool connected with a specific product automatically gives a client user access to the **Shared** pool of unassigned licenses.

License access is defined per user pool, not per client user. You assign a specific license capacity (either for specific product features or specific products) for check out by users of the pool. You can also restrict a user pool from check out operations or block all check out operations for a specific pool. For details on restricting or blocking user pools, see ["Restricting or Blocking User Pools" on page 107](#)

For details on creating user pools and assigning licenses to a user pool, see ["How to Manage Client User Access" on page 109](#).

License Usage by User Pools

After creating user pools, you can reserve a certain amount of license capacity to each user pool. This is done in the **Feature-Based** and **Product-Based** Reservation tabs. For details, see ["Featured-Based/Product-Based Reservation Tab" on page 116](#).

Each pool is assigned an amount of license capacity as decided by the AutoPass License Server administrator or Product Administrator. The reserved capacity can exceed the currently available installed capacity. However, license requests from a client user that exceed the installed capacity of the feature or product (even if they are less than the reserved capacity of the user pool) are not fulfilled.

In order to fulfill these requests, you need to install additional licenses or borrow licenses from another AutoPass License Server. For details on installing additional licenses, see ["Installing Licenses" on page 71](#). For details on borrowing licenses, see ["Borrowing Licenses" on page 73](#).

When you assign license capacity to each pool, you limit the license capacity available for check out to the users in that pool. License requests from client users that exceed the reserved capacity of a pool are not fulfilled.

Note: If a client user is part of another user pool, the AutoPass License Server also checks the other user pools (based on priority order) to see if other pools have available capacity to fulfill a check out request). For details, see ["License Reservation Priority" on page 106](#).

If a user's request exceeds a pool's reserved capacity, the AutoPass License Server can also fulfill the request by combining capacity from a user pool with available capacity from the *Shared* pool. The AutoPass License Server does not fulfill check out requests by combining available capacity from multiple user pools.

¹A group of client users which receives access to specific licenses as defined by the License Server administrator(s).

Note: Restricted pools cannot combine with the *Shared* pool to fulfill a user request.

In addition, the available installed capacity is consumed on a first-come, first-serve basis, regardless of priority order. If the first request comes from a lower-priority pool, the request is fulfilled.

Examples

In this example, there are three user pools, and the available capacity for a feature is 150, as detailed below:

Pool Name	Reserved Capacity	Restricted/Blocked	Installed Capacity
Pool1	100	No	330
Pool2	50	No	
Pool3	30	No	
Shared	200	N/A	

Use Case 1

A client user in *Pool3* makes a check out request for a capacity of 30. This request is fulfilled, even though *Pool3* is the third pool in the list.

Use Case 2

A client user in *Pool1* makes a check out request for a capacity of 150. Since the reserved capacity for *Pool1* is not sufficient to fulfill this request, the AutoPass License Server combines the capacity available in *Pool1* with available capacity in the *Shared* pool to fulfill the check out request.

Use Case 3

A client user in *Pool2* makes a check out request for a capacity of 300. Normally, the AutoPass License Server would combine the available capacity of 50 in *Pool2* with the available capacity in the *Shared* pool to fulfill the request. However, since the request exceeds the combined capacity of 250 (between *Pool2* and the *Shared* pool), the request is not fulfilled until additional licenses are installed or borrowed.

License Reservation Priority

After creating user pools, you can set the priority order for user pools to access licenses. Thus, if a client user belongs to multiple pools, license requests are fulfilled by taking available capacity from the user pools in a set priority order. The priority order also decides the order in which user pools have access to licenses for check out.

Set the priority order for each feature by dragging the user pools listed for each feature or product in the Feature-Based or Product-Based Reservation tabs.

Examples

In the following examples, there are two client user pools, *Pool2* and *Pool3* (set in priority order), as well as the *Shared* Pool, as seen below:

Selected Feature : 10624:1 Available Capacity: 100 Total Capacity: 100			
	Allow/Block	Pool Name	Reserved Capacity
<input checked="" type="checkbox"/>	Block	Pool2	25
<input checked="" type="checkbox"/>	Block	Pool3	50
<input checked="" type="checkbox"/>		Shared	25
		Total	100

Use Case 1

The client user belongs to both *Pool2* and *Pool3*. If the client user sends a check out request for a capacity of 10, the AutoPass License Server tries to fulfill the check out request from *Pool2* based on priority order.

Use Case 2

The client user belongs to both *Pool2* and *Pool3*. If the client user sends a request for a capacity of 60, the AutoPass License Server tries to fulfill the request first by checking the available capacity in *Pool2*. In this scenario, since *Pool2* and *Pool3* do not have adequate capacity, the license request is fulfilled by combining the higher priority *Pool3* with the Shared pool to complete the license request.

Feature-Based vs. Product Based Reservation

When you reserve licenses for user pools, you can assign licenses in two different ways:

- **Feature-Based Reservation:** This type of reservation makes licenses available only for specific features within a product. Other product features are not available to client users with a feature-based license.
- **Product-Based Reservation:** This type of license enables a client user to have access to all product features.

The available capacity for a feature is dependent upon the capacity reserved for the product. For example, if you reserve a capacity of 50 for *ProductA* in one user pool, all the features of *ProductA* have a capacity of 50 available for check out by members of the user pool.

You do not have to reserve the same capacity for all features of a product as are reserved for the product itself. Thus, you can reserve a capacity of 40 for a user pool for Feature 1 of *ProductA*, even if the user pool has a capacity of 50 reserved for *ProductA*.

For example, if you want a client user to have access only to specific environments or configurations in a particular product, you reserve licenses using feature-based reservation. If you want a client user to have access to all product features, use product-based reservation.

Allotting features within a product for feature-based reservation is done on a per-product basis. For details on license types and license allotments for products, see the individual product documentation.

Restricting or Blocking User Pools

In addition to limiting the available license capacity for check out, you can also restrict or block user pools from performing check out operations.

Restricting¹ a user pool limits the user pool's ability to check out licenses by limiting the available capacity for check out to only the reserved capacity of the pool. When a pool is restricted, client users cannot combine the available capacity in a user pool with the *Shared* pool to fulfill their license requests.

Example

In this example, the installed capacity of a feature is 100. There is one user pool with a reserved capacity of 40. The shared pool has an available capacity of 60. If a client user sends a check out request for a capacity of 60, the request response is received as seen below:

Pool Names	Reserved Capacity	Installed Capacity	Requested Capacity	Response for Unrestricted Pool	Response for Restricted Pool
Pool1	40	100	60	Request is fulfilled in combination with the <i>Shared</i> pool.	Declined due to insufficient capacity.
Shared	60				

Blocking² a user pool prevents a user pool from performing any check out operations. By selecting the **Block** option for a user pool, all check out operations are prevented and the reserved capacity of the pool is set to 0.

¹Limiting the ability of a user pool to combine with the Shared pool to fulfill license check out requests that exceed the reserved capacity for a user pool.

²Preventing a user pool from checking out any licenses for a feature or product.

Selected Feature : 10624:1 Available Capacity: 100 Total Capacity: 100			
	Allow/Block	Pool Name	Reserved Capacity
<input checked="" type="checkbox"/>	Block	Pool2	<input type="text" value="35"/>
<input checked="" type="checkbox"/>	Allow	Pool3	<input type="text" value="0"/>
<input type="checkbox"/>	Block	Pool4	<input type="text" value="15"/>
<input checked="" type="checkbox"/>	Block	Shared	<input type="text" value="50"/>
	Block	Total	<input type="text" value="100"/>

This option is useful if you want to prevent a particular user group from checking out licenses for a feature, but still allow that group to access other features or products. Since all created user groups are displayed in the Feature-Based and Product-Based Reservation tabs and are therefore available for license reservation, blocking a user group enables you to prevent a user from reserving licenses for a user pool.

Note: Using the **Block** option for a user will block only the selected pool. However, if the user belongs to a different pool which is not blocked, the AutoPass License Server can fulfill the request based on available capacity in the other pools.

Tasks

How to Manage Client User Access

This task describes the procedures necessary to manage client users and user group access to the AutoPass License Server.

This task includes the following steps:

- ["Add a user pool" below](#)
- ["Add a user pool" below](#)
- ["Remove a client user's attribute from a pool" on the next page](#)
- ["Reserve product license capacity to a user pool" on the next page](#)
- ["Reserve feature license capacity to a user pool" on the next page](#)
- ["Set the user pool priority order for feature license checkout" on the next page](#)
- ["Block a user pool" on page 111](#)
- ["Restrict a user pool" on page 111](#)

Add a user pool

1. In the Pool Management tab (Reservation Management pane), click the button.
2. In the Create New Pool dialog box, enter a name and description for the user pool.
3. Click **Create**.

The user pool is displayed in the user pool list in the Pool Management tab (Reservation Management pane).

Note: You can later delete user pools by clicking the **Delete** button .

Add users to a client user pool

1. In the Pool Management tab (Reservation Management pane), select the radio button for the pool to which you want to add client users. The lower pane displays the selected pool name.
2. In the lower pane, select a client user attribute to add. You can enter the client user's **User Name**, **IP Address**, **Host ID**, or **Client ID**.

Note: It is recommended (although not mandatory) to enter all available attributes for a client user in the user details. Although a client user does not have to have all attributes included in the user group's details, if a client user tries to access the AutoPass License Server without having all attributes in the pool's attribute list, the client user cannot access the server. For details, see ["Client User Attributes" on page 103](#).

3. Click **Add**



The user's details are displayed in the Associated Users area of the lower pane.

Remove a client user's attribute from a pool

1. In the Pool Management tab (Reservation Management pane), select the radio button for the pool from which you want to remove client users.
2. Click **Remove** .

The client user's attribute is removed from the user pool.

Note: Removing a user's attribute from the pool does prevent a user from accessing the AutoPass License Server. As long as the other client attributes match with the attributes stored in the AutoPass License Server, the client user can continue to access the server.

Reserve product license capacity to a user pool

1. In the Product-Based Reservation tab (Reservation Management pane), select the product to reserve from the drop-down menu.

Note: All features for the product are also displayed.

2. In the user pool table, reserve a capacity to the available pools.

Note: There is no shared pool for product-based license reservation.

3. Click **Submit**. The feature table is updated to reflect your reservations.

Reserve feature license capacity to a user pool

1. In the Feature-Based Reservation tab (Reservation Management pane), select the product from the drop-down menu.
2. In the feature table, select the radio button for the feature for which you want to reserve capacity. The lower pane displays the feature name and information and the available user pools.
3. In the Reserved Capacity column of the lower pane, reserve a capacity to the available pools.

Note: All unreserved available capacity is automatically assigned to the *Shared* pool.

4. Click **Submit**. The tables in both the lower and upper panes are updated to reflect your reservations.

Set the user pool priority order for feature license checkout

1. In the Feature-Based Reservation tab, select the product for which you want to set user pool priority order.
2. Select the radio button for the feature for which you want to set user pool priority order.
3. In the User Pool Feature Details area, drag the row containing the user pool up or down until the priority is set in the correct order.

Block a user pool

1. In the Feature-Based Reservation or Product-Based Reservation tabs (Reservation Management pane), select the product for which you want to block a user pool's check out operations.
2. If you are in the Feature-Based Reservation tab, select the feature.
3. In the lower pane, click **Block** for the user pools you want to block and click **Submit**.

The capacity of the selected user pools is changed to 0 and the user pool's name is displayed in the upper pane (of both the Feature-Based and Product-Based Reservation tabs) with a (r) next to the pool name.

Note: To enable a user pool, click **Allow**. The previously reserved capacities are restored.

Restrict a user pool

1. In the Feature-Based Reservation or Product-Based Reservation tabs (Reservation Management pane), select the product for which you want to restrict.
2. If you are in the Feature-Based Reservation tab, select the feature.
3. In the Restrict column of the lower pane, select the check box for the user pools you want to restrict.
4. Click **Submit**.

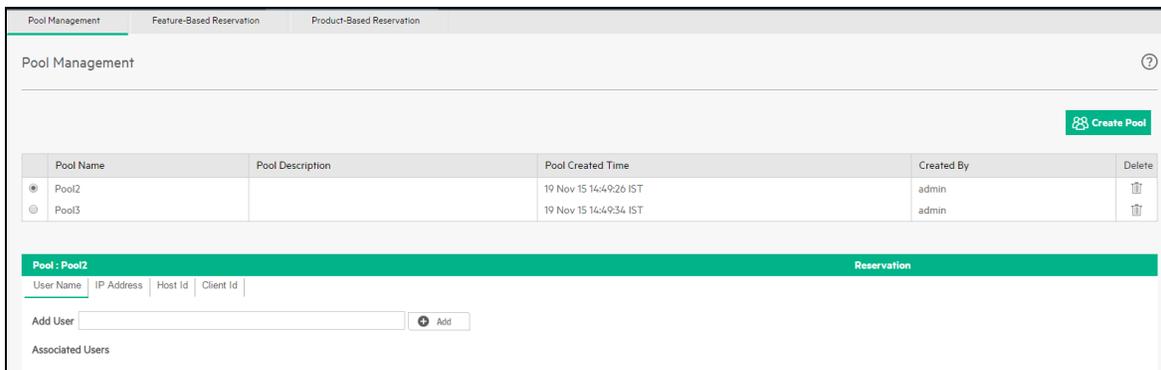
The feature or product table is updated with a (r) next to the feature or product's name. The reserved capacity remains the same.

Note: To clear the restriction, clear the check box for a user pool and click **Submit**.

Reference

Pool Management Tab

This tab enables you to create user pools and add users to user pools.



To access	Reservation Management pane> Pool Management tab
Important information	You must create a user pool before adding client users.
Relevant tasks	"How to Manage Client User Access" on page 109
See also	<ul style="list-style-type: none"> • "Pool User List Section (Pool Management Tab)" on the next page • "Pool to Product Mapping List (Pool Management Tab)" on page 115 • "AutoPass License Server Client User Pools" on page 104 • "License Server Client Users - Overview" on page 102

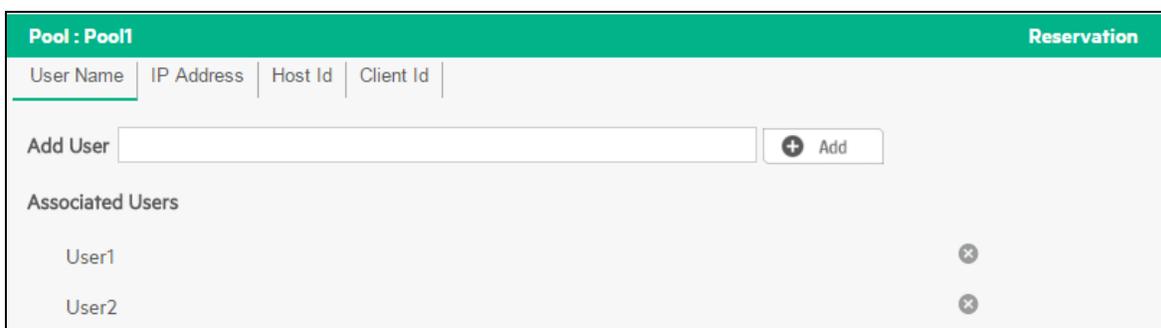
User interface elements are described below:

UI Element	Description
	Opens the Create New Pool dialog box, in which you give a name and description for a new user pool.
Pool name	The user pool name given to a user pool by the AutoPass License Server administrator.
Pool description	The description of the pool entered when creating the pool. Use a description that enables you to identify the purpose of a specific user pool.

UI Element	Description
	<p>Note: It is not mandatory to enter a description for a user pool.</p>
Pool Created Time	The date and time of the pool's creation.
Created By	The AutoPass License Server administrative user or product administrator user that created the user pool.
	<p>Delete. Removes the user pool.</p> <p>Note: If a pool is deleted when a floating license is checked out from the pool, then the checked out capacity will reflect under common pool and the same is displayed in In Use graph.</p>

Pool User List Section (Pool Management Tab)

This section enables you to add client user attributes to a user pool.



To access	In the Pool Management tab (Reservation Management pane), select the radio button for a user pool.
Important information	<ul style="list-style-type: none"> Pool user details displayed in this window are dependent upon the user pool selected in the Pool Management tab. It is not necessary to enter all user attributes for each client user. However, entering all attributes for each client is recommended (if they are available).
Relevant tasks	How to Manage Client User Access
See also	<ul style="list-style-type: none"> Pool Management Tab Pool to Product Mapping List (Pool Management Tab) Client User Attributes

User interface elements are described below:

UI Element	Description
User Name	<p>The Windows or Unix user name of a client user.</p> <p>This field supports all special characters and is both case sensitive and insensitive.</p> <p>Refer "Configuring Case Insensitivity" below for more details on case insensitivity.</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <p>Note: The user name must use the following syntax: DOMAIN/USER NAME</p> </div>
IP Address	<p>The IP address of the computer from which the client user accesses the AutoPass License Server.</p>
Host ID	<p>The host address for the computer the client user uses to access the AutoPass License Server.</p> <p>To find the host address for the client user's computer, enter <code>ipconfig/all</code> in the Command Prompt window. The Host ID is the host name with the DNS suffix displayed in the results.</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <p>Note: The Host ID must use the following syntax: <HOST NAME>.<DNS SUFFIX>.</p> </div>
Client ID	<p>A unique value for each client user.</p>
	<p>Add Attribute. Adds an attribute to the user pool after you enter the information in the edit field.</p>
Associated Users/IPAddresses/Host ID/Client ID	<p>The list of Users, IP Addresses, Host IDs, or Client IDs that have been added to the user pool.</p>
	<p>Remove. Removes an client user's attribute from the user pool.</p>

Configuring Case Insensitivity

The option of switching from case sensitivity to case insensitivity is provided with the help of the property mentioned below in Config.xml file available in the path

<APLS Data Folder Path>\data\conf

<Entry key="com.hp.autopassj.ls.reservation.group.case_insensitive.allowed">true</entry>

To allow case insensitivity set the flag "true". By default it is set to "false" which means that it accepts only case-sensitivity.

Pool to Product Mapping List (Pool Management Tab)

This page enables you to view information on the products and features reserved for a specific user group.

Product	Feature
10027_1.0_HP UFT_12.50	10618:1

To access	In the Pool Management tab (Reservation Management tab), click the Reservation button in the Pool User List section (lower pane).
Relevant tasks	How to Manage Client User Access
See also	<ul style="list-style-type: none">Pool Management TabPool User List Section (Pool Management Tab)Feature-Based vs. Product Based Reservation

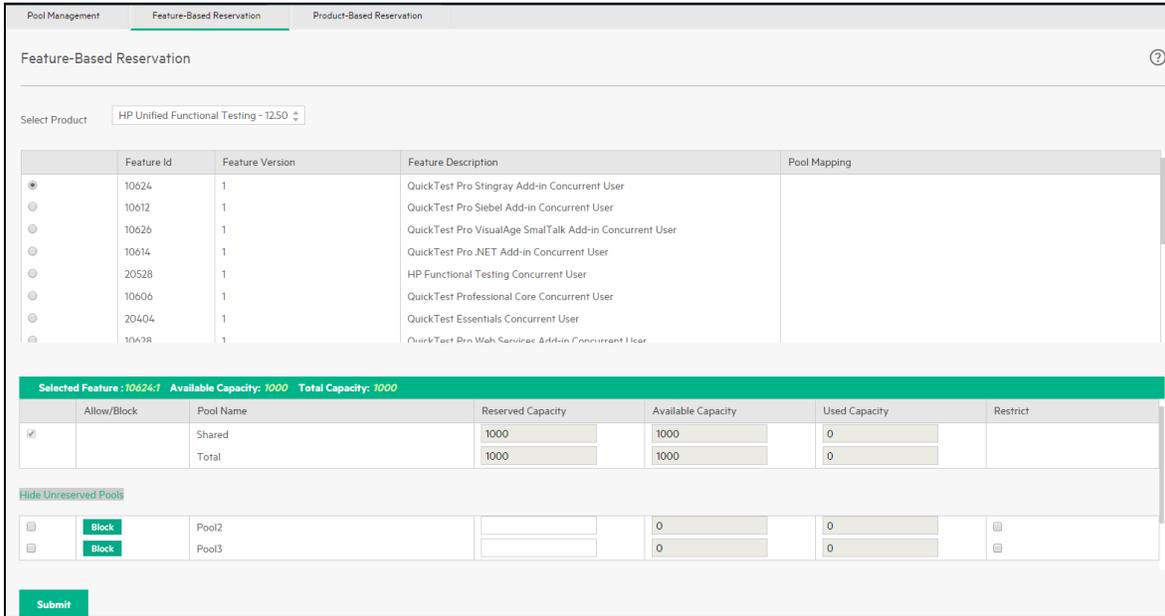
User interface elements are described below:

UI Element	Description
Pool name and description	The name of the user pool whose reservations are currently displayed.
Product	The products for which this particular user group has license capacity reserved.
Feature	The features for which this particular user pool has license capacity reserved.

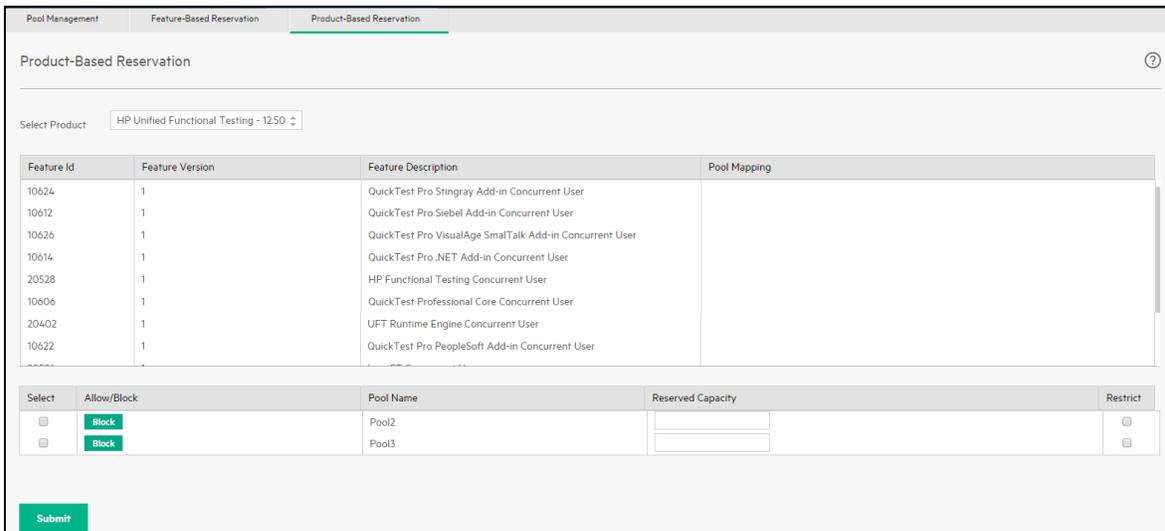
Featured-Based/Product-Based Reservation Tab

This tab enables you to assign license capacity for product features.

The image below shows the Feature-Based Reservation tab.



The image below shows an example of the Product-Based Reservation tab.



To access

In the Reservation Management pane, select the Feature-Based Reservation or the Product-Based Reservation tab.

Important information

You must reserve capacity for a product before reserving capacity for its features.

Relevant tasks	"How to Manage Client User Access" on page 109
See also	<ul style="list-style-type: none"> • "Feature-Based vs. Product Based Reservation" on page 106 • "Restricting or Blocking User Pools" on page 107 • "License Reservation Priority" on page 106 • "License Usage by User Pools" on page 104

User interface elements are described below:

Feature/Product List Table

UI Element	Description
Feature ID	The feature's unique identification.
Feature Version	The feature's version number.
Feature Description	A textual description of the feature.
Pool Mapping	<p>A listing of the user pools and corresponding capacities mapped to these user pools. For example, for a <i>FeatureA</i>, the pool mapping is displayed as <i>Pool1:20</i>, <i>Pool2:15</i>, and so on.</p> <p>If a pool is restricted or blocked, the pool name is displayed with an <i>(r)</i> next to the pool name.</p>

User Pool Feature/Product Reservation Details Area

UI Element	Description
<feature details>	<p>The details for a particular feature. These details include:</p> <ul style="list-style-type: none"> • Selected Feature: The feature name • Available Capacity: The capacity currently available for checkout • Total Capacity: The total installed capacity <p>Note: The reserved capacity for a user pool can be greater than the available capacity or total capacity. However, check out requests that exceed the available capacity are declined.</p>
Block / Allow	Disables or enables the ability of a user pool to perform check out requests for a specific feature.
Reserved Capacity	<p>The license capacity reserved for members of this pool. All check out requests less than the reserved capacity are fulfilled automatically.</p> <p>If a check out request exceeds the reserved capacity, the client user can combine the available capacity in this pool with the <i>Shared</i> pool to complete a check out request.</p>
Available Capacity	The capacity currently available for a check out request.
Used Capacity	The capacity currently checked out.
Restrict	When this check box is selected, the client users in the selected user pool can fulfill only those check out requests which do not exceed the available capacity for the feature.
Hide/Show Unreserved Pools	Hides or shows user pools that are unreserved for the selected feature.

Client User Management - Frequently Asked Questions

The following are frequently asked questions about managing client users and user pools in the AutoPass License Server.

Can a client user access product or feature license capacity without being assigned to a user pool?

No. Client users are added as part of a user group following the creation of a user pool. There is no way to independently add a user without first placing the user in a user pool.

When adding a client user, do I have to enter all four attributes for a client user?

No. However, it is recommended to do so. If the user tries to check out a license from the AutoPass License Server later with a User name, IP address, Host ID, or Client ID that is not an associated attribute for the user's pool, the check out request is denied.

Can a user's license request be fulfilled if the user pool in which the user is a member does not have enough available capacity?

Yes. If there is not enough available capacity, the client user can fulfill the request by taking the available capacity from the user pool and combining it with available capacity in the *Shared* pool.

Can I reserve license capacity for multiple features or products at a time?

No. You can reserve capacity only for a single feature or single product at a time. However, you can reserve licenses for a single feature or product for multiple user groups simultaneously.

How does the AutoPass License Server select a pool to fulfill a license request if a client user is part of multiple user pools?

The AutoPass License Server selects the user pool from which to check out the license based upon the priority order of the user pools for a feature or product.

If there are multiple pools with reserved capacity for a feature, and a lower priority pool makes the first check out request, is the request fulfilled?

Yes. License check out requests are fulfilled on a first-come, first-serve basis.

If I want to limit a client user's ability to check out licenses, how to I do this?

You have two options for restricting check out:

- You can restrict the user pool, which limits check out requests to only the reserved capacity in the pool. For details, see ["Restrict a user pool" on page 111](#).
- You can block a user pool, which prevents all check out requests. For details, see ["Block a user pool" on page 111](#).

Can a license be checked in by a client user in a blocked pool?

Yes.

How do I check from which pool I check out licenses?

In the License Usage pane, select the Feature ID for which you have checked out a license. The Pool field displays the pool name to which the license belongs.

Client Users Management - Troubleshooting and Limitations

The following are frequently asked questions about problems encountered while managing client users and user pools in the AutoPass License Server.

Why is a client user unable to check out licenses?

A client user cannot check out licenses for one of the following reasons:

- The client belongs to a user pool that is blocked. For details, see ["Restricting or Blocking User Pools" on page 107](#).
- The client user belongs to a restricted user pool and the requested capacity is not available for that pool.
- The request capacity is not available for that feature.

Chapter 11: Remote Commuter License Management

This chapter includes:

Concepts

- ["Commuter Licensing - Overview"](#) on the next page
- ["Commuter License Check In and Check Out"](#) on the next page
- ["Recovering Commuter Licenses"](#) on page 124

Tasks

- ["How to Perform Remote Commuter License Operations"](#) on page 125

Reference

- ["Check In/Check Out Tab \(Remote Commuter Pane\)"](#) on page 127
- ["Remote Commuter Licensing Management - Frequently Asked Questions"](#) on page 129
- ["Remote Commuter Licensing Management - Troubleshooting and Limitations"](#) on page 130

Concepts

Commuter Licensing - Overview

At times, client users need to use a licensed product without a connection to the AutoPass License Server to check out a license. Normally, the lack of a connection to the AutoPass License Server would prevent the user from checking out a license and thereby prevent them using the product. However, users without a connection can use a **commuter license**¹ to use a product without a connection to the AutoPass License Server. For example, client users that travel frequently with limited or no access to the AutoPass License Server benefit from commuter licenses.

A commuter license is checked out from the License Server and is later installed on the client user's computer (when there is no active connection to the AutoPass License Server). The commuter license enables the product to open and run without a connection to the AutoPass License Server. After the client user is finished with the license, the user checks it in to the AutoPass License Server.

Note: The user only needs to be connected to the AutoPass License Server during license check in and check out.

Once a commuter license is checked out from a product or feature's capacity, the capacity remains checked out until the license is checked in or expires.

Unlike live concurrent licenses, you cannot revoke a commuter license.

Each product or feature can enable or prevent commuter licenses. This can be done by the product itself through the license key or you can set the settings for commuter license usage in the Feature Report for a particular feature. For details on setting commuter licenses in the license key file, see individual product documentation.

Commuter License Check In and Check Out

In order to receive a commuter license, you or the client user must check out a commuter license. Commuter license check out is done in one of two ways:

- **Direct:** The client user connects directly to the AutoPass License Server and checks out the license. For details on performing this type of check out, see the individual product documentation.
- **Remote:** An AutoPass License Server user checks out the license and sends it to the client user.

Only users with administrator privileges can check out commuter licenses for all products and features. Product Admin users can check out licenses for the associated products in the User Groups tab (User Management pane).

Before checking out a remote commuter license, each client user must generate a file in the client system. This file contains the license requirements for the client's program and the client computer details. For details on generating this input file, see the individual product documentation.

¹A license that allows a user to use a product without an active connection to the License Server.

To check in a remote commuter license, the user also needs to generate an file in the client computer. This output file contains the license details and the client computer's information. When checking in the license, this enables the AutoPass License Server to recognize the commuter license.

All AutoPass License Server users can check in a remote commuter license.

Recovering Commuter Licenses

On occasion, a commuter license is lost before it is used by a client user. This happens when:

- A mail server goes down when sending the license key via email
- The downloaded license key file is corrupt
- The AutoPass License Server user navigates to a different page in the AutoPass License Server after checking out a license but before downloading the license key.

Using the Feature Report page, you can download the license file again and use it in a client user's program.

Tasks

How to Perform Remote Commuter License Operations

This task describes the processes necessary to manage commuter licensing operations.

This task includes the following steps:

- ["Enable commuter licensing " below](#)
- ["Modify commuter licensing settings" below](#)
- ["Check out a commuter license" on the next page](#)
- ["Check in a commuter license " on the next page](#)
- ["Recover a commuter license" on the next page](#)

Enable commuter licensing

1. In the License Usage pane, select the feature for which you want to enable commuter licensing.

Note: A feature that allows you to enable commuter licensing is displayed with a cleared, enabled check box next to the Feature ID.

2. Click **Manage Commuter**.

The License Server displays a message confirming the commuter license enabling and the feature is displayed with a checked, enabled check box.

Modify commuter licensing settings

1. In the License Usage pane, click the **Feature ID: Version** link for the feature for which you want to modify commuter licensing settings. The Feature Report page for the feature opens.
2. In the Feature Report page, in the Commuter Checkout Settings section, click **Edit**.
3. Enter the **Maximum number of days allowed** for a commuter license checkout and the **Maximum capacity allowed** for a check out operation.
4. Click **Save**.

The Feature Report page displays the modified values for the commuter license settings.

Note: If you do not enter a value for the Maximum capacity allowed, all the available capacity is set as the maximum capacity for check out.

Check out a commuter license

1. In the Check Out tab (Remote Commuter pane), click the **Browse** button and navigate to the file generated in the client computer for commuter license check out.
2. Click **Check Out**.
3. In the Check Out page, select the features to check out and click **Download Link**.

The license key file is downloaded and is available for use by a client user.

Note: If you want to exclude certain features from a particular commuter check out, select the features in the Check Out page and click **Discard**.

For details on installing the license in a client computer, see the individual product documentation.

Check in a commuter license

1. In the Check In tab (Remote Commuter pane), click the **Browse** button and navigate to the file generated in the client computer for the commuter license (as described in "[Commuter License Check In and Check Out](#)" on page 123).
2. Click **Check In**.

The license is checked into the AutoPass License Server and the capacity is added to the available capacity displayed in the License Usage pane.

Recover a commuter license

1. In the License Usage pane, select the feature for which you want to recover a commuter license and click the **Feature ID: Version** link. The Feature Report for that page opens.
2. In the Feature Report page, click the **Remote/Commuter** link in the license details table.

Note: You can download a commuter license only if it is not checked in.

3. Save the file to a convenient location.

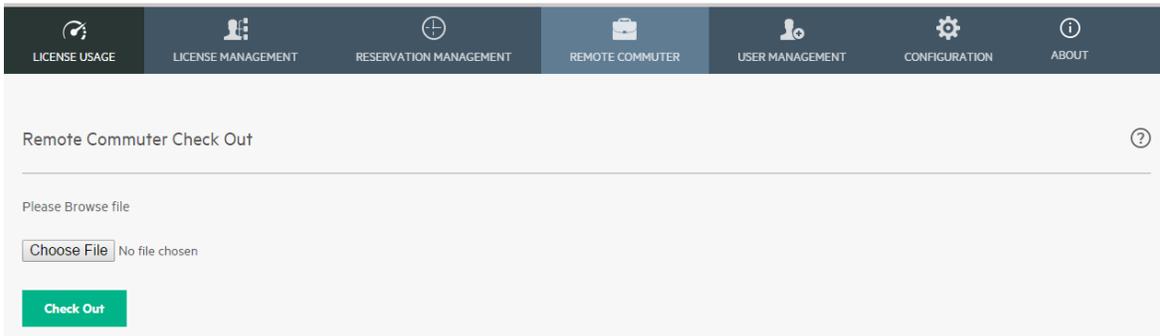
Note: The commuter license capacity listed as checked out does not change after downloading a commuter license again.

Reference

Check In/Check Out Tab (Remote Commuter Pane)

These tabs enable you to select the features for a commuter license check out or check in.

The image below shows an example of the Check Out pane.



To access	Remote Commuter pane > Remote Commuter Check Out/Remote Commuter Check In tab
Important information	In order to check out a commuter license for the feature, a feature must have commuter licensing enabled, as displayed in the License Usage pane or the Feature Report page. For details, see License Usage Pane and Feature Report Page (License Usage Pane) .
Relevant tasks	"How to Perform Remote Commuter License Operations" on page 125
See also	<ul style="list-style-type: none"> • "Commuter Licensing - Overview" on page 123 • "Commuter License Check In and Check Out" on page 123 • "Recovering Commuter Licenses" on page 124

User interface elements are described below:

UI Element	Description
<file path>	The path to the output file generated in the client user's system for commuter license check out/check in.
Browse	Opens a dialog to enable you to find the output file for commuter license check out/check in.

UI Element	Description
Check Out Check In	Opens the Check Out/Check In page, in which you select the features for commuter license check in or check out.

Remote Commuter Licensing Management - Frequently Asked Questions

How can I tell if a product or feature is enabled for a commuter license check out?

In the License Usage pane, a product or feature is shown as enabled for commuter license check out in the following ways:

- It has a selected, disabled check box next to the Feature ID.
- It has a selected, enabled check box next to the Feature ID.

If a feature allows commuter check out but the commuter check out is not yet enabled, the check box is displayed as a cleared, enabled check box. Select the feature's checkbox and click **Manage Commuter** to enable a commuter license check out.

Who can check out a commuter license?

Only users with *administrator* or *Product Admin* access privileges can check out commuter licenses. Product administrators are limited to check out of commuter licenses for the associated products in their user groups.

Who can check in a commuter license?

All AutoPass License Server users can check in a commuter license.

Why is there an option to download a commuter license?

This option is used to recover a commuter license that is lost. Instead of performing license cleanup and checking out the licenses again to recover these licenses, a AutoPass License Server user can download the licenses again using the Feature Report page for the feature.

Why am I not able to checkout Commuter/Remote Commuter from License Server?

There are two reasons why commuter/remote commuter checkout is not allowed,

- If the feature is restricted for commuter/remote commuter checkout, then you will not be able to do these two types of checkout. In case of UFT, by default all features are enabled for commuter checkout; however APLS admin can change this by clicking "Manage Commuter" with selected features (in License Usage) to disable the commuter checkout.
- If the client and AutoPass License Server are in the same system. Commuter is restricted for clients in the same system as AutoPass License Server as client doesn't require to get offline licenses (commuter/remote commuter) in this case.

Remote Commuter Licensing Management - Troubleshooting and Limitations

The "Product is not configured with this AutoPass License Server" error message is displayed when checking out a commuter license. Why?

This error message indicates that a product is not configured in the AutoPass License Server. Check out a live or commuter license to configure a product and then check out a remote commuter license.