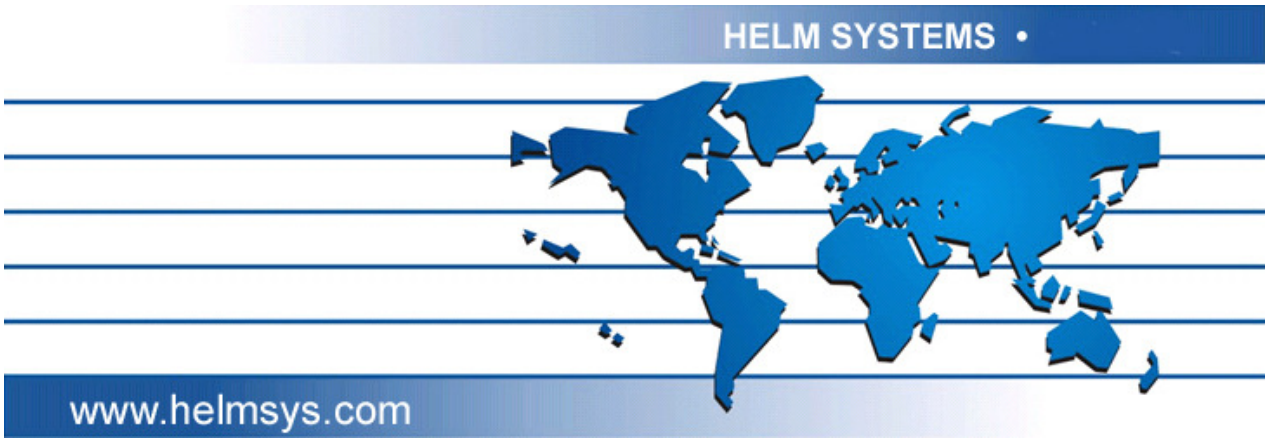
RAP Clientless SSL Web Portal

Administrator Manual



Helm Systems

Table of Contents

Table of Figures

1. Introduction

This Server Administration Manual will explain the web-interface of the RAP (Remote Access Pass) Server Administration Console to set-up, enable, and manage the RAP service by the server administrators so that RAP users have a functional and reliable interface for access to their registered computers. Before we go to the details of the manual for the RAP administration, let us first get familiar with what RAP is and how it is working.

The RAP allows RAP users to remotely control their registered computers. In addition the RAP will enable your users to gain remote access to their remote files, directories, and applications with any internet-ready PC.

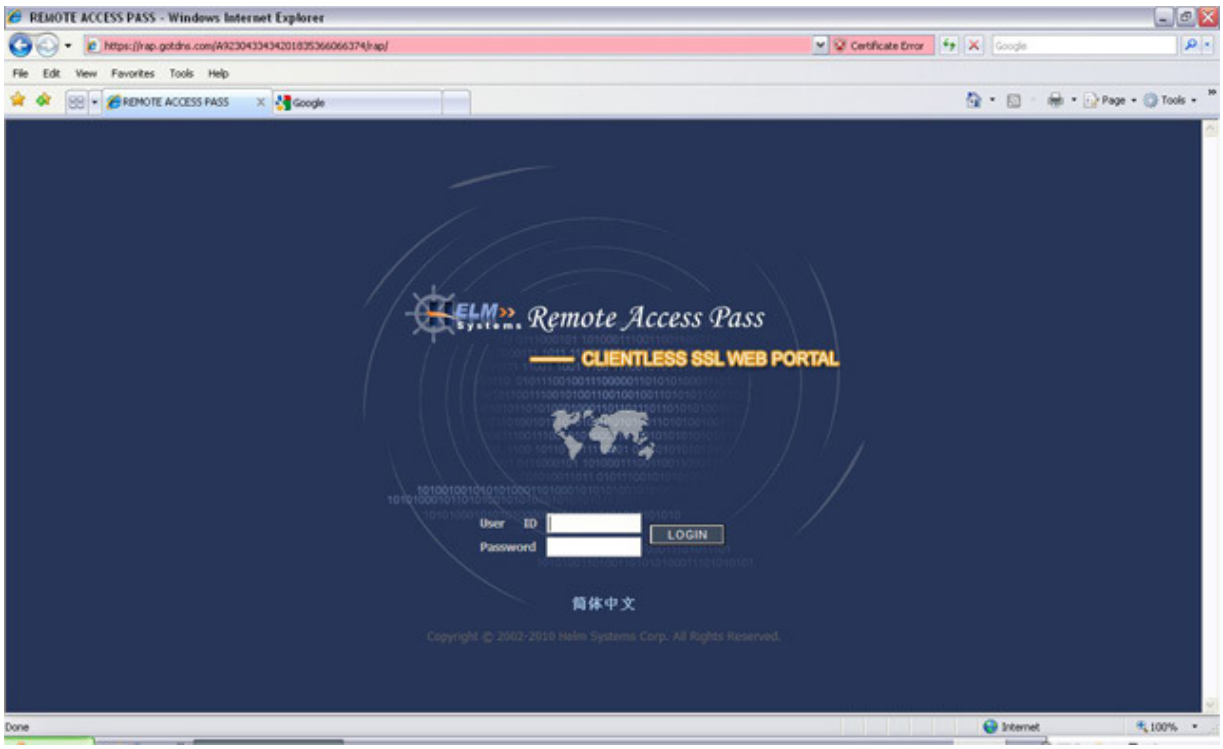


Figure 1: The Application Login Page

Figure 1 shown above is the primary **end-user** interface obtained from the RAP server after a secure log-in. From this screen the user may make several requests and changes to personal information on the central site server. Following figure 2 shows the application main functionality page to make some concept to manage it for RAP administrator.

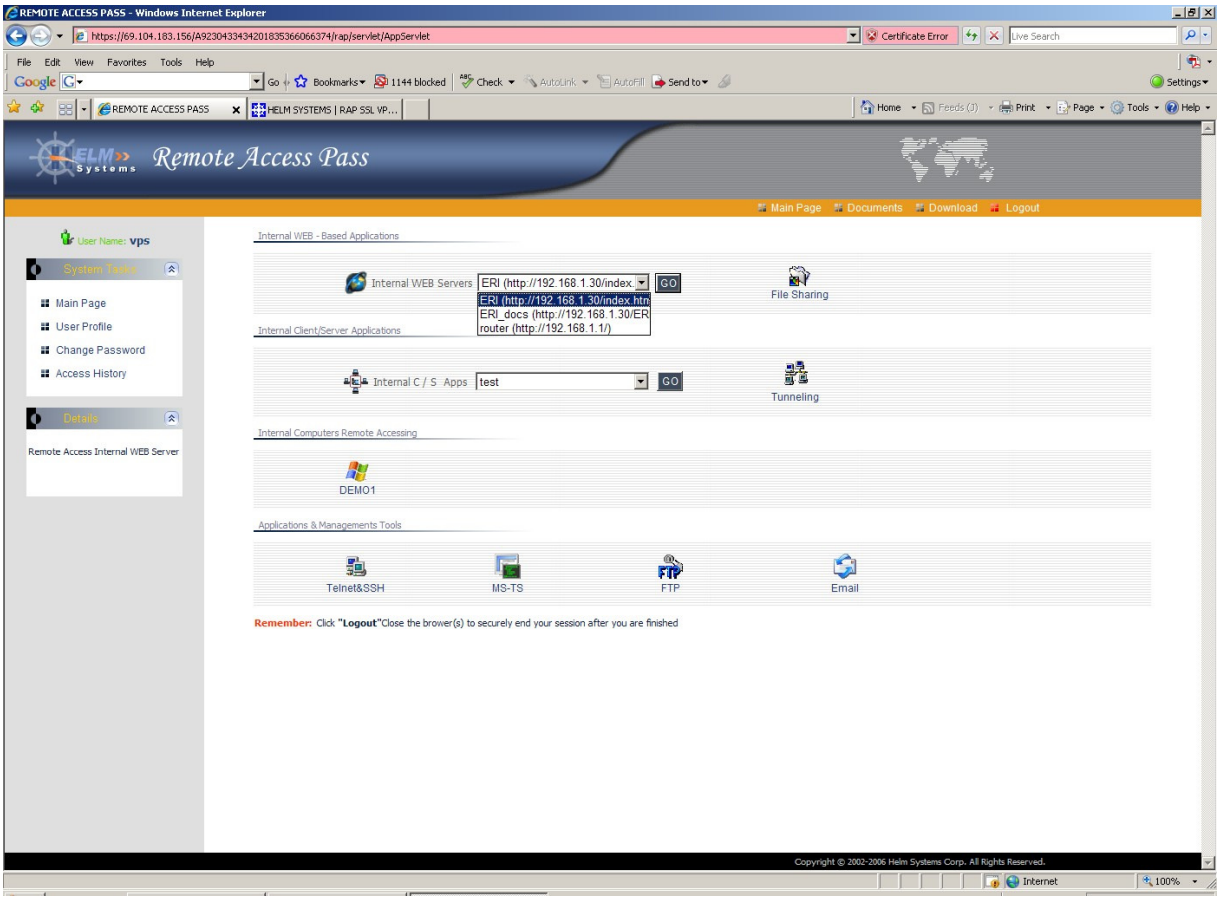


Figure 2: Application Main Page

2. RAP Server Administration System

2.1 Login

The RAP Server Administration system is administered from a trusted IP address (if specified) and a unique User ID and password. The 8802 port is default used as admin console port. The initial UserID and Password are "Admin" and "helmsys".

Login uses HTTPS to send a User ID and password that may be changed through a pre-determined management port also protected by the definition of a trusted IP domain and network mask settings. User ID is case-sensitive and may begin with a letter or number, though spaces and special characters are not allowed.

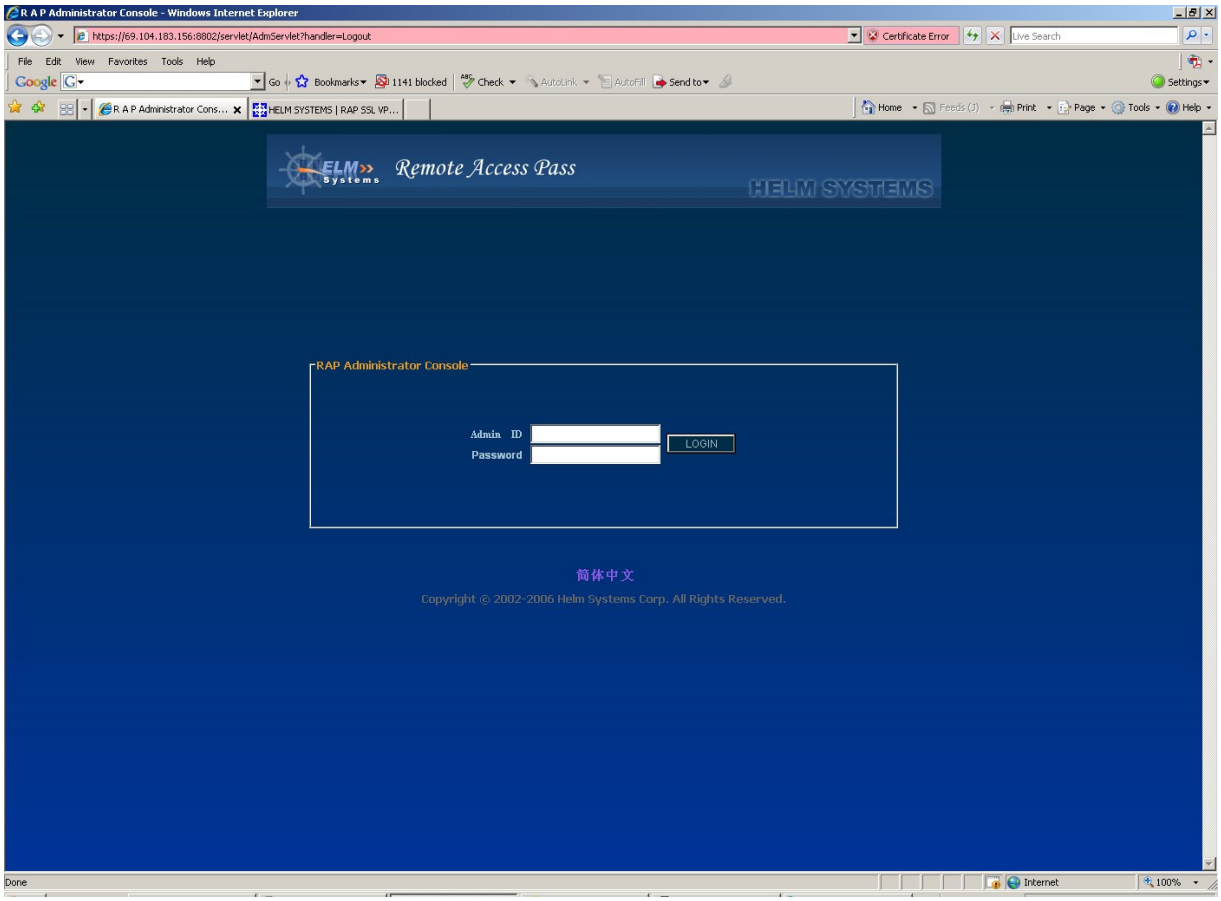


Figure 3: RAP Server Administration login interface

Only the correct User ID / password, directed at the correct port, and sent from the specified trusted domain will be granted access to the Admin console.

After login, a view with tabs (System, Users and Targets) for different management tasks will appear in the left-hand frame.

3. System Manager

3.1 System Setting

The "System Setting" link on the System tab allows you to set the System IP, the Domain name, the Gateway IP, and the DNS IP. Proper configuration of the system is required for any operation. Once the system is functioning these settings should not have to be changed.

CAUTION: Once set up properly any changes to the system configuration or the server settings may disable the service.

Figure 4: System Configuration

Modify both "Trusted IP" and "Trusted Mask" to limit which IP or IP domain can access the admin console. ex. 192.168.1.50 and 255.255.255.254 to make 192.168.1.50 can access admin URL only.
Clicking the "OK" button on any tab sends the changes to the Central server.

NOTE: If Mail Server is setup, the user can get the temporary password from email when that user is added to RAP. Otherwise, Administrator need tell the temporary password to each new user following the info of display.

3.1.1 Enable NAT

When RAP is deployed as bridge in the topologic of the internal network, you should setup the route to make connection work between different network interfaces. Select NAT "enabled". Since SSL delivery eliminates the NAT and firewall traversal issues encountered with traditional remote access products, allowing your remote users reliable and ubiquitous access from external networks are the biggest advantage for SSL. Using NAT is not a good solution of RAP.

3.1.2 Update Root CA for Two-way SSL

If the two-way SSL authentication is required, select the "Client Authentication" either "Enable" or "Want". And update the users root CA to click "Update root CA" link.

If the browser in the client side has a legal certificate match this root CA, then login RAP automatically even do not need to enter password.

Configure the file sysconfig.xml: Add tag parameter <CRL>"CRL server name"</CRL> so that RAP retrieves the message from CRL to check if the certificate exists.

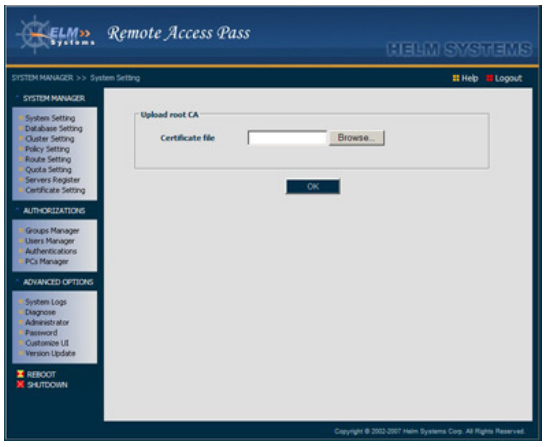


Figure 5: Update Root CA

3.1.3 Other Network Interfaces configuration

Click "Configure Other Network Interface" can view the all enabled network interfaces except the main interface in the "System Configuration" page.

Click each of the name of card link can modify the parameters of the interface

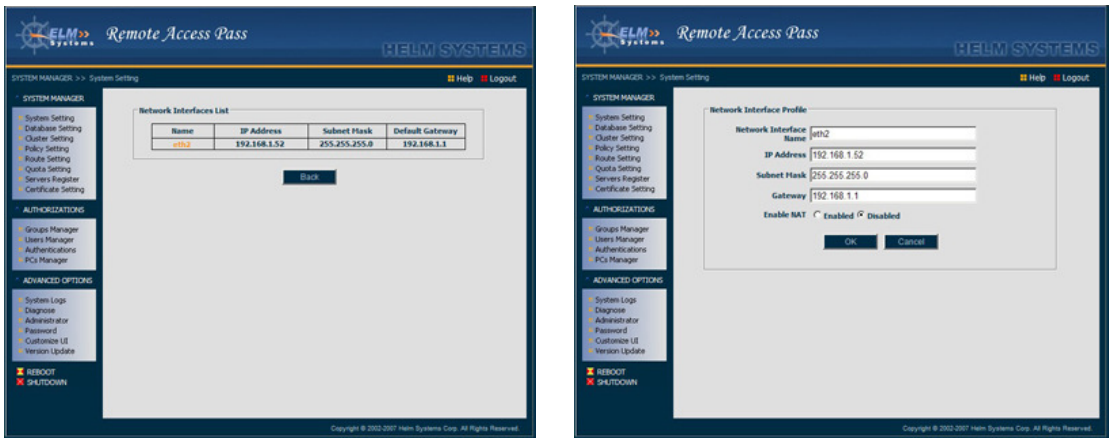


Figure 6: Other Network Interfaces Configuration

3.1.4 Timeout Setting

Click "Timeout", can set the time following three kinds of sessions:

1. The RAP admin session time.
2. The RAP application session time.
3. The user applications can be accessed session time.

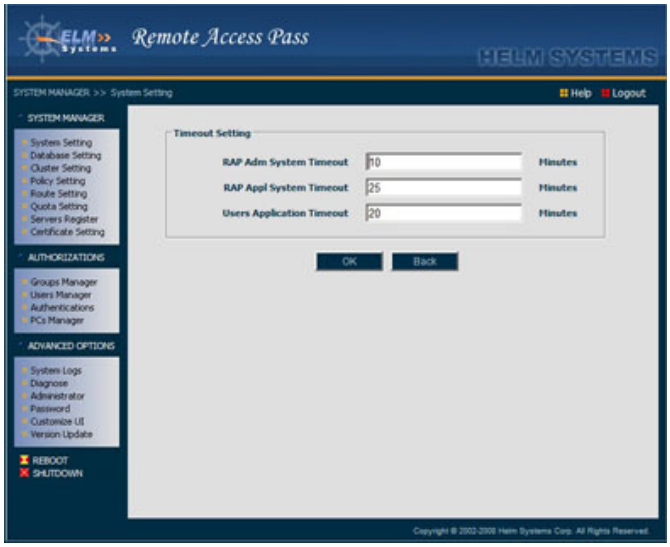


Figure 7: Timeout Setting

3.1.5 System Time Setting

Click "System Time", can set the system time selecting from the calendar and clock.

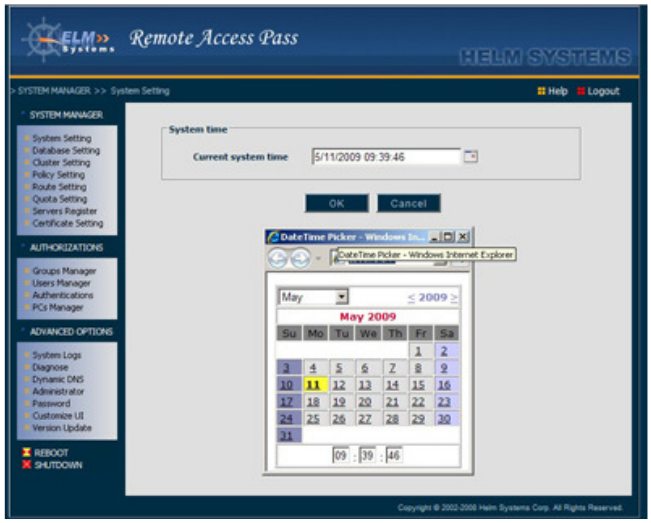


Figure 8: System Time Setting

3.2 Database Setting

Select a DB type for this RAP. The default DB type of single RAP is “Embedded”.

- Embedded: use local DB and do not allow the other RAP access to this DB through network (do not allow modify the URL)
- Embedded Network Service: use the local DB and allow the other RAP access to this DB as a central DB (do not allow modify the URL)
- HSQL: The central DB is HSQL, replace the host from the specific IP address
- MYSQL: The central DB is MYSQL, replace the host from the specific IP address
- If uses other DB like Oracle, SQL Server, can ask the provider to initialize the DB using RAP’s script files of the initial data. The URL can be edited in the URL field following the initialed format.
- External password encryption algorithm can replace default algorithm when you set the flag :
  - ✓ <EXTERNAL_CRYPTO_ALG>Y</EXTERNAL_CRYPTO_ALG> <CUSTOMER_CRYPTO_KEY></CUSTOMER_CRYPTO_KEY> in sysconfig.xml
  - ✓ Put external algorithm code in an jar file to folder /usr/apps/tomcat/shared/lib
  - ✓ The API must following: class name: com.amity.crypto.Encryptogram;
  - ✓ Function name:

    String encryptOp(String input, String encrypt_key);
    boolean checkPassword(String clear_password, String encrypt_password, String customer_crypto_key).

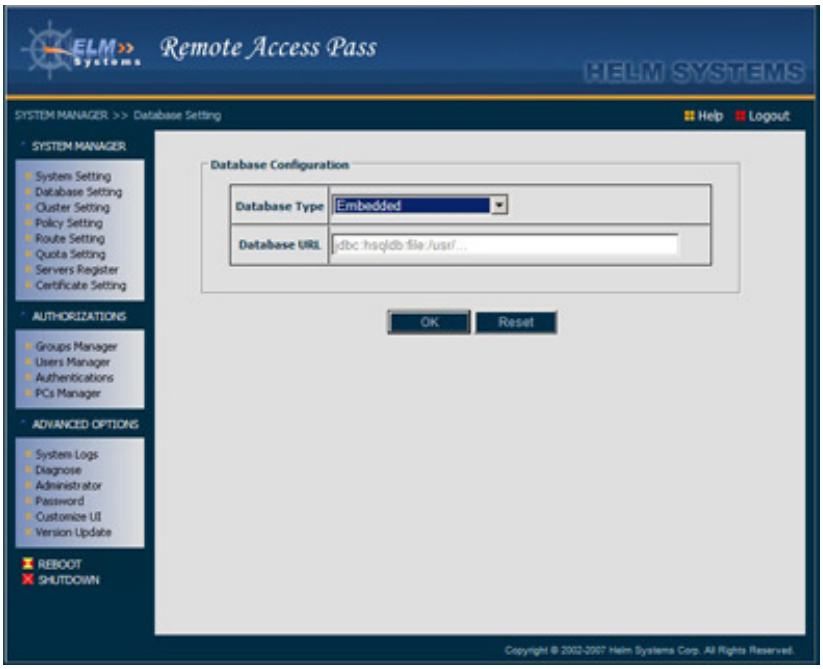


Figure 9: Database Setting

3.3 Cluster Setting

Check “Enable” in checkbox of the Cluster Setup and reboot RAP to make clustering enable.

3.3.1 Cluster

This RAP is a normal member in the cluster. Inputs the name of the domain of the cluster to make sure the message can be sent or received to the all members (same domain name) only in this cluster. Inputs the banded IP (normally the RAP system IP) that should be a physical IP as well as does not allow mapping IP makes communication using the port 8012 of this banded IP in TCP protocol between members within the cluster. The port 8015 of this banded IP in UDP protocol send message to every members.
There are different registered users in different RAPs when uses the cluster. For example: The user1 registered in RAP1. The RAP1 is down during the user1 login to the RAP1. The user1 can switches to the RAP2 automatically and does anything as same as in RAP1. The condition is the user1 must login to RAP1 first before user1 can login to RAP2.

3.3.2 HA

The two RAPs connect in the LAN using cluster mode can implement HA function.

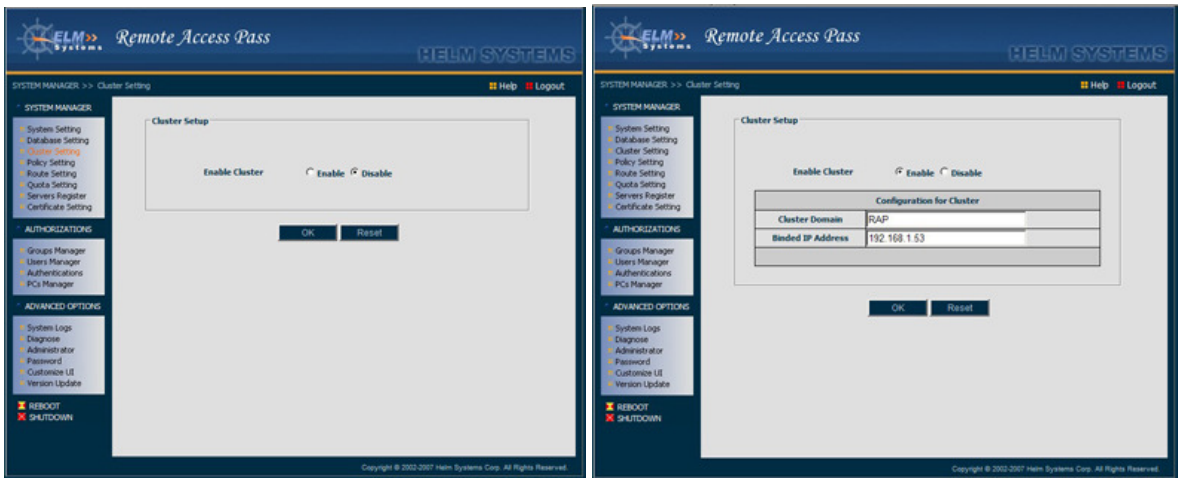


Figure 10: Enable and Configure Cluster

3.4 Policy Setting

You can add or delete policies to set the RAP has different levels protection. The policy setting is similar to configuration of policy of a firewall. "Policy Setting" feature corresponds to "Tunneling" server accessing mode.

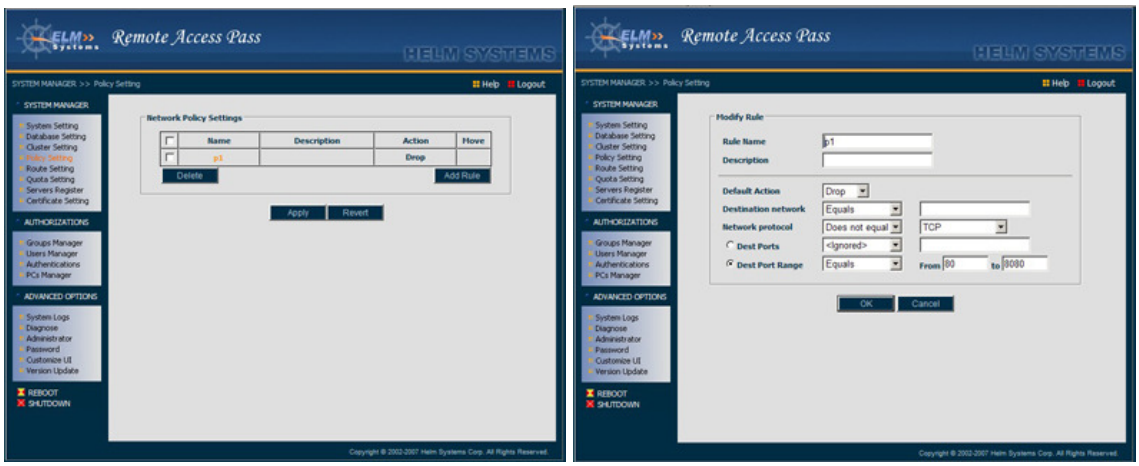


Figure 11: Policy Setting

When user sets the policy of firewall in the RAP box, such as open some ports (original setting to open 443, 80, 8802, 139, 445 ports). You can edit the script file to add the policy of firewall: /usr/apps/tomcat/data/default.sh.

3.5 Route Setting

Add or delete static route tables to change the default route table.

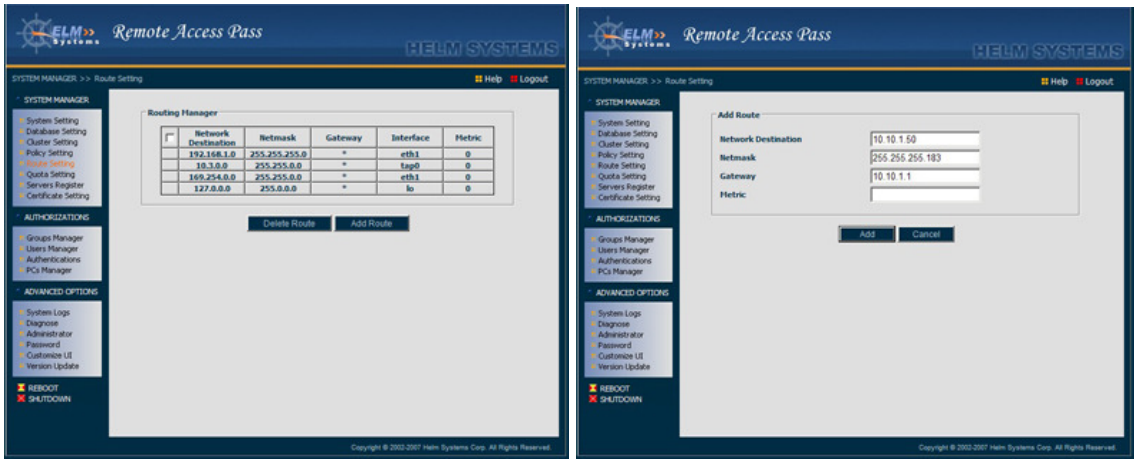


Figure 12: View and Add a Static Rout Table

3.6 Quota Setting

The "Quota Setting" all administrators watch what situation on current RAP system and three kind of limit quota number. When RAP need to add quota number, you can email to RAP customer support and get new secret string number.

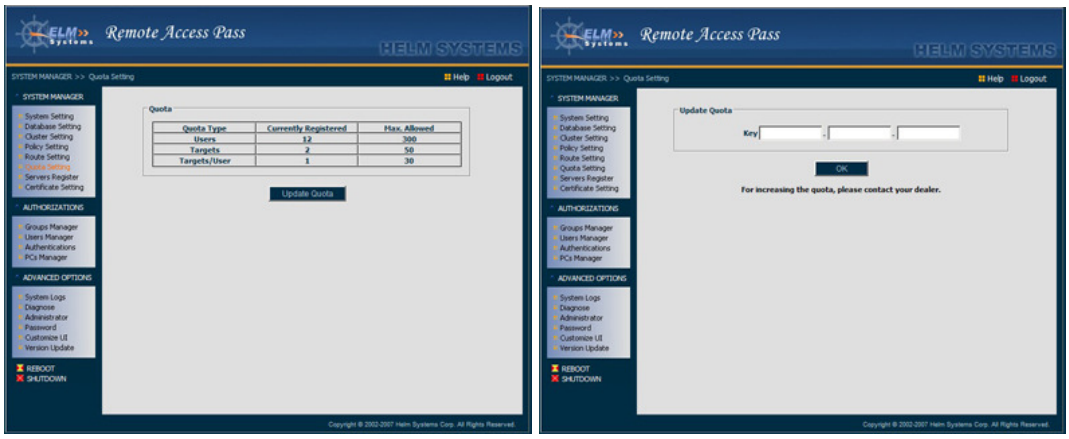


Figure 13: View and Update Quota

When you get the new serial number from Helm Systems, you can click "Update Quota" to enter the new serial number to modify the maximum allowed concurrent users.

3.7 Servers Register

- From the Servers tab, internal server types can be viewed.
- Select a server type, which can be added and deleted.

Figure 14: The Internal Server Types List

Figure 15: Servers List

3.7.1 Web Based Server and MS Exchange Server for Web Server

Internal Web Servers is meaning internal web based application servers deployed in the LAN:

A selection can link a URL of web based application server in the servers list. User can click the "Go" button to connect this server.

3.7.1.1 WEB servers

There are two type web based servers:

- MS Exchange Outlook Web Access
- General web based server

3.7.1.2 Process for internal or absolutely URL in the page of server

- Extra Link: These internal URLs can be linked each other in this web server must be added this text area. (Each URL in the text area separated by "Return" one by one and these URLs do not display in the server list in application).
- It must add http:// or https:// prefix in text field of Server URL, when WWW type server is selected. The other servers just enter the IP address in the URL field.
- Exchange server configuration is similar Web server's

3.7.1.3 Process for URL register when SSO

- To make SSO usable, the server URL must be set following format:

  http://x1.x2.x3.x4/login_page (http://192.168.1.10/login.htm)
  ?uid=%RAP_SSO_USER%&pwd=%RAP_SSO_PASSWORD%

3.7.1.4 Interface requirement for authentication in user side when SSO

- The login part of application server needs to set to authentication:

  String userId = req.getParameter("uid");

  String passwd= req.getParameter("pwd")

3.7.1.5 URL accessing control

- Filter and block the sub folders under the main URL using white list and black list. This is a pure application layer switch that controls accessing of applications in the intranet.

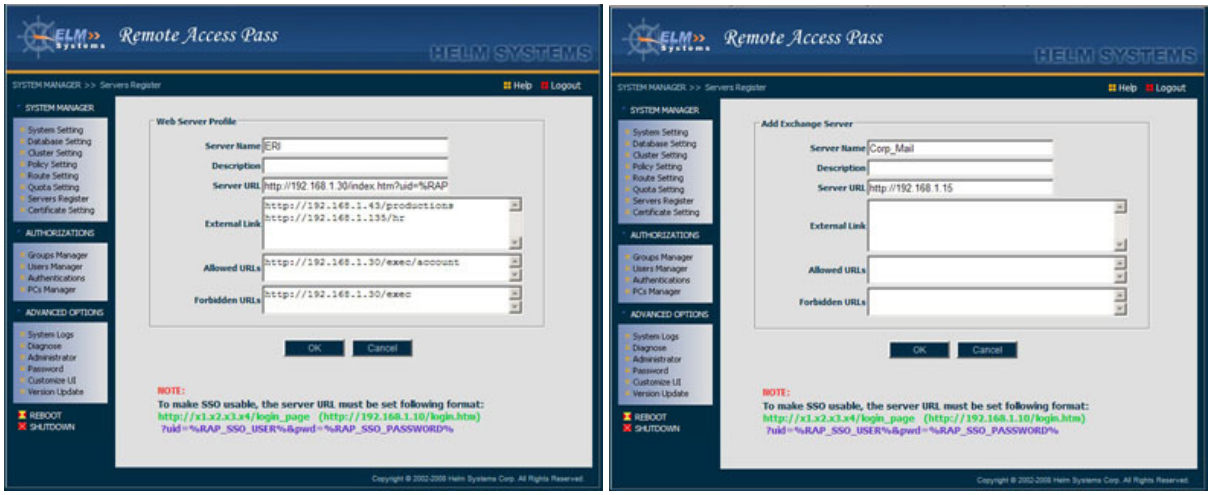


Figure 16: Web Server and Exchange Mail Server

3.7.2 Applet to support well-known protocol

Telnet, SSH, MS Terminal Service, FTP, POP3 and IMAP set that server URL and ports. (JRE is needed to download automatically)

FTP service supports both passive mode and active mode

All above type of servers are set fixed IP

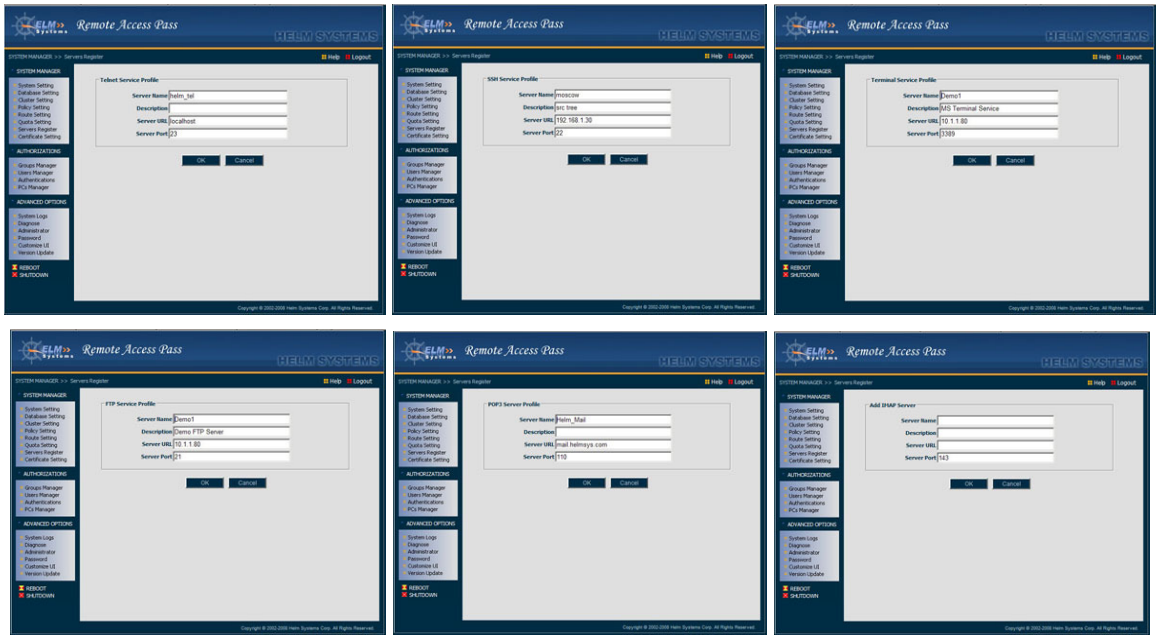


Figure 17: Telnet, SSH, MS-TS, FTP, POP3 or IMAP server

3.7.3 Restricted Client / Server (Java Applet)

This is a good way to access the application of client / server:

- The application uses fixed ports only.
- Client side can be installed JRE (for fixed location is more better since it does not need to download and install JRE)
- The IP connection in the configuration of client software of user can be redirected

  Server Port: only one port can be input. (JRE is needed to download automatically)

  Extra TCP Ports and UDP Ports can input more than one separated by ";"

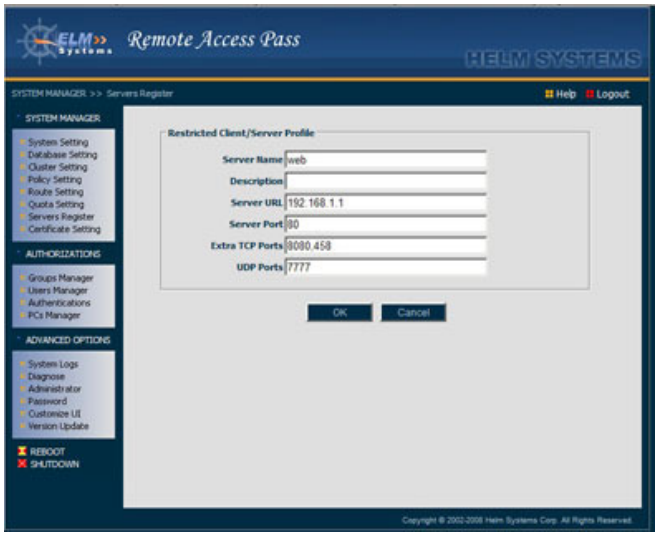


Figure 18: Restricted Client / Server

3.7.4 Generic (Layer3) Client / Server (Windows ActiveX)

When user tries to select this type service to access internal client/server application, it needs download and run a client side package. The taskbar of the remote PC display icon "", Right click this icon select "Exit" to tune off this agent.

Besides support specific ports as well support dynamic ports application. This mode does not have to register any application IP or ports so that it supports and cases of TCP/UDP level applications. It only need to give "Allow" or "Forbidden" the phase of IP for TCP or UDP to make sure which protocol of the IP can be allow through RAP.

Format: <host>[/mask>]:[<port>][<port2>]

- The switch of accessing Internet during remote C/S connection is built up

  When uncheck the "Allow Internet Access" checkbox, Internet can be accessed when the agent is running.

  When check this checkbox, only the IP allowed passing RAP can be accessed.

- The admin can pre-register the web based servers or some URLs of Internet line by line to allow user access them directly

Format: <display_name>=<url> (GOOGLE=http://www.google.com)

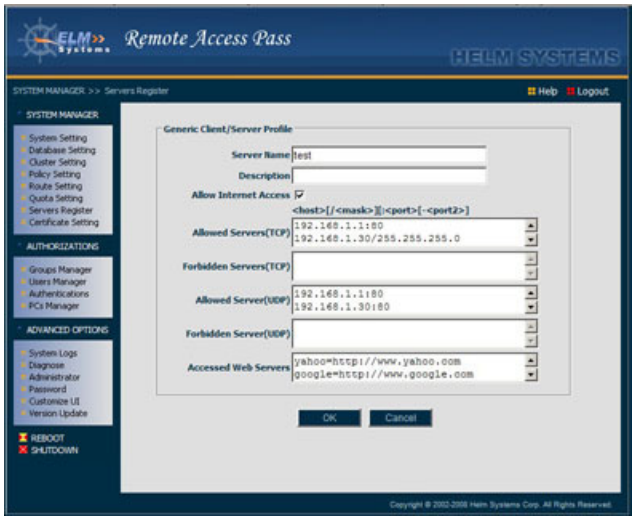


Figure 19: Generic Client / Server

3.7.5 Tunneling

This is an IP over TCP mode, which needs download both JRE and a small agent. When there is any application bellow TCP level need be accessed, this mode is a selection like IPSec VPN.

It does not need any specific port be configured on the firewall.

DHCP IP range set: Start IP, End IP, and Subnet Mask

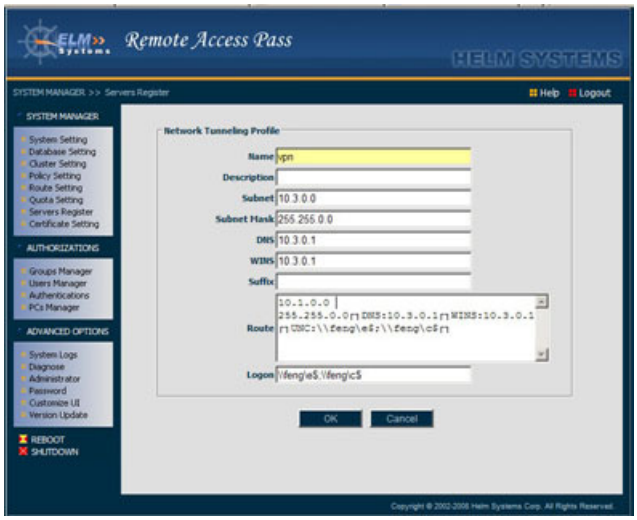


Figure 20: Tunneling

3.8 Certificate Setting

3.8.1 Sets Server Certificate

Update a new certificate to the RAP server. The user can upload a exist certificate as well as generate a new certificate. The new certificate is stored in Key Store: vpstore and load it from local PC to the RAP

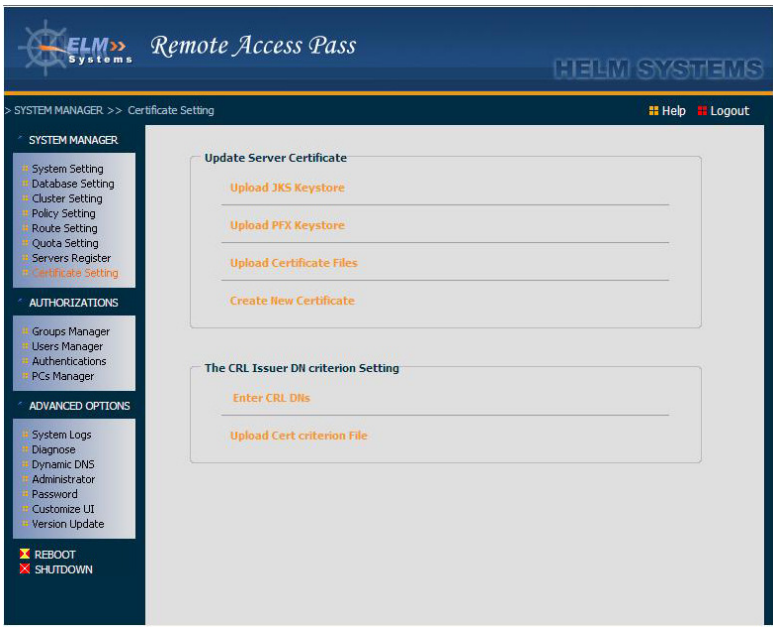


Figure 21: Update Certificate

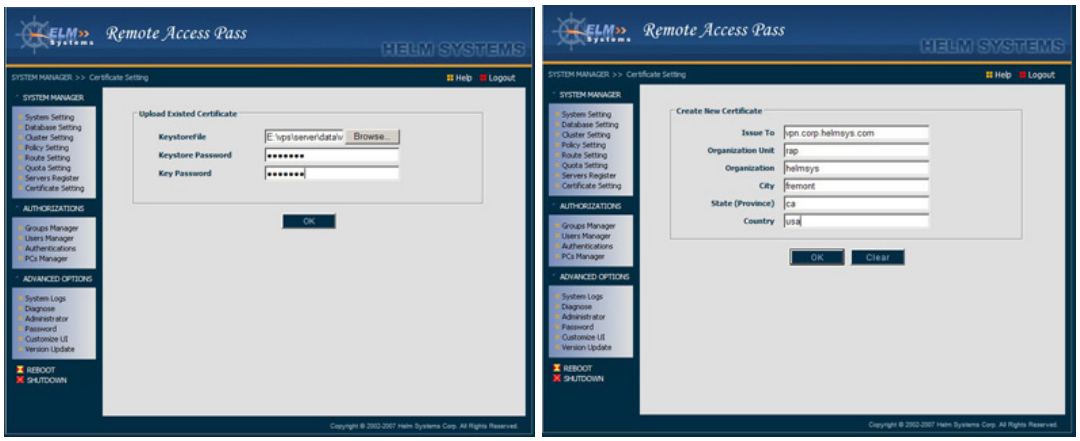


Figure 22: Upload and Create Certificate

3.8.2 Sets CRL Search Criterions

Inputs Issuer DN(s) or uploads the certificate .cer file(s) that include issuer DN issued by user to search the CRL{s} located in the non default node in the LDAP server when enable both TWO-WAY SSL and CRL checking.

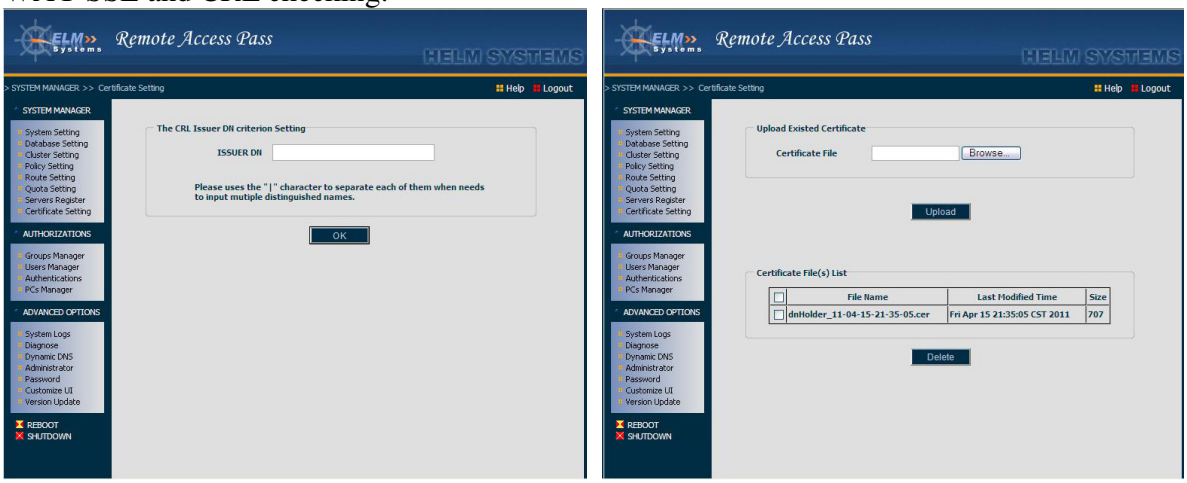


Figure 23: Input ISSUER DN or Upload Certificate include ISSUER DN of user

- The DN inputted must follow X500Name format, For example: CN=RAP, O=helmsys Each DN must be separated by "|" when inputs multiple DNs to support multiple CRLs.

- Upload .cer certificate file(s) that included ISSUER DN issued by user if the ISSUER DN inputted does not match the user issued DN.

  Multiple CRLs mode is supported after upload multiple .cer certificate files.

  The file(s) selected can be deleted.

The ways above can not be used at same time!

4. Authorizations

4.1 Groups Manager

- Groups List: Admin can add a new group or delete a group and display the groups list
- Modify Group Data: Make it enable or disable.
- Enable or disable the File Sharing functionality.
- Enable or disable the Remote Control desktop functionality.
- Enable or disable the other well known protocol applications such as Telnet, SSH, FTP, MS Terminal Service and Email (transfer native protocol to http protocol) functionality.
- Click "Customize" to set accessing servers right for this group
- Click "Add User to Group" to add users from current user list to this group

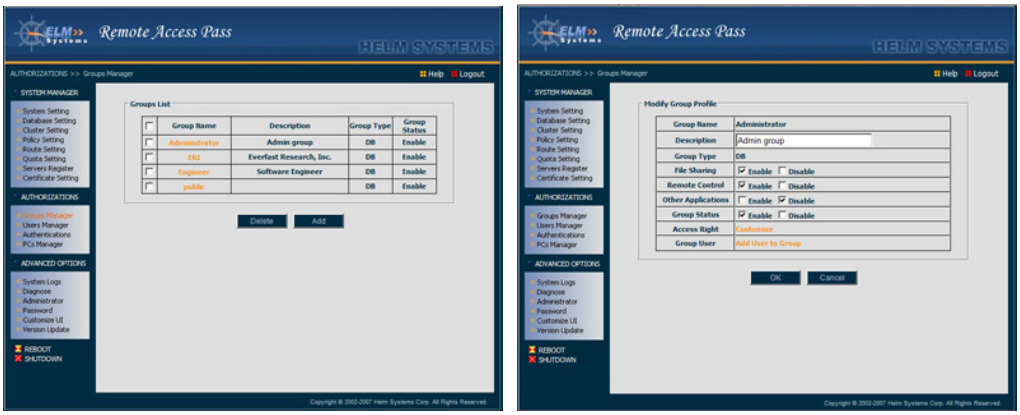


Figure 24: Groups List and Group Data

Figure 25: Access Servers Privileges

4.2 Users Manager

4.2.1 Users List

- The Users tab shows all registered users within the system. Ten User IDs and User names are shown at a time. Additional pages of users may be viewed by selecting the page number links at the bottom the page.
- Enter User ID in the search field to find the target user and gets the user profile.

Figure 26: User Manager

- Click "Delete" to delete the users who had been selected in the check boxes.
- Click "Add" to add a new user who can receive a welcome email.
- Click "Export" to backup all the users' information in the database to a saved file.
- Click "Online User" to monitor the users who are using RAP system as well as can enforce to interrupt the users current connections.

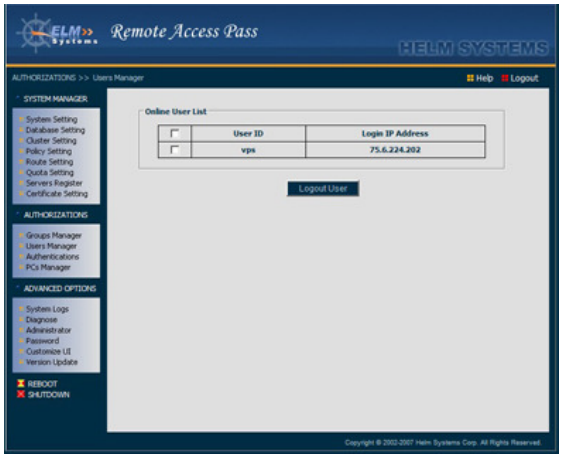


Figure 27: Online User Monitor

- Click "Set Filter" to select a category and type keyword in the field in the filter page to display sorting by grouping.

Figure 28: Search in Category

4.2.2 User Profile

- Selecting a specific user link shows the registered Full Name, E-mail address, Mobile Number, Enable/Disable account toggle check boxes and the number of registered target computers. Any changes to the fields are made when the OK link is selected.

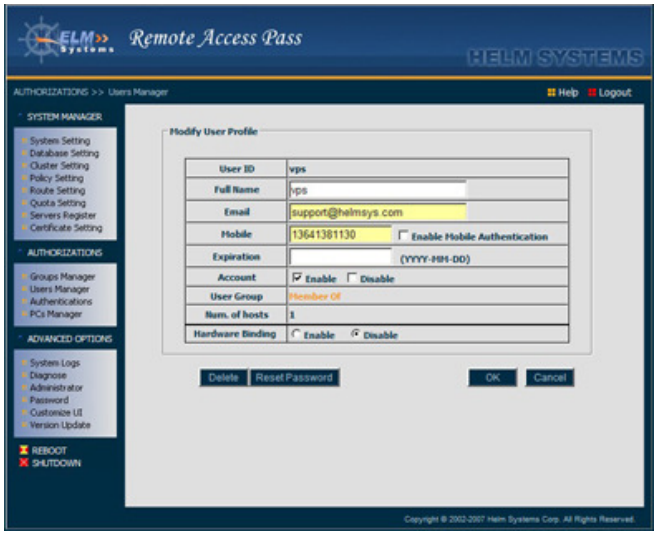


Figure 29: Modify User Profile

- To reset the password for an individual user, select the User ID link for the user who requires the reset and then use the link to "Reset Password", An automatic e-mail notice will be sent to the end-user or display on the next page with the newly reset password randomly generated by the server.
- User Profiles may be deleted from the system by checking the boxes in the left-hand column and then selecting the Delete link at the bottom of the column.
- Click the "Member Of" link, to assign the user to groups

Figure 30: Assign user to groups

- Selecting a link from the Computers column will display the computer(s) registered to the user in the row selected. The User Name, Host ID, and the Host name are displayed. Subsequently selecting the Host ID displays the Target Computer Profile in the left-hand frame. The system administrator can make no changes except deletion to the Target Computer Profile. The user may modify this information from the "User Profile" link on the "Main Page" page.

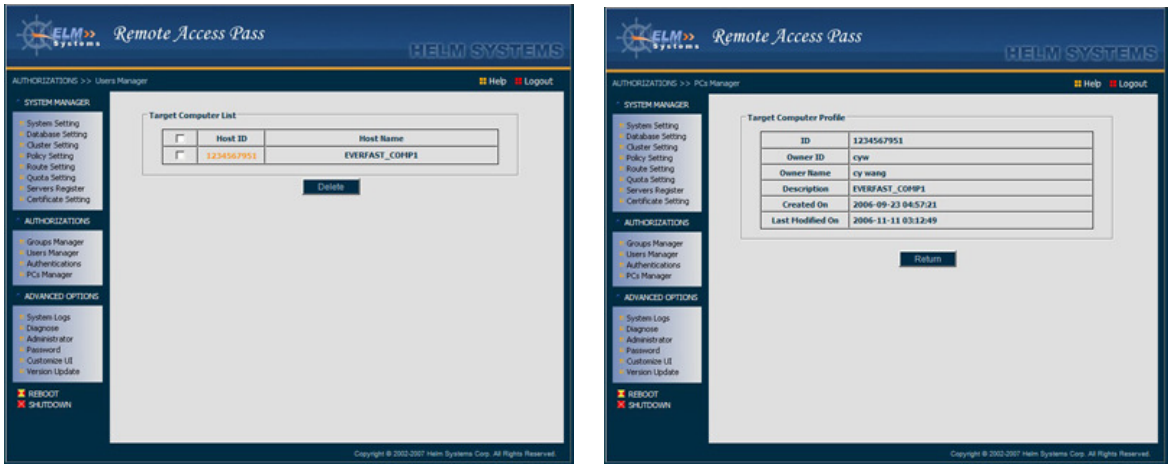


Figure 31: The User Own Target Computer

4.3 Extra Authentications

- Admin can select authentication type which user used
- Select a certificate from USB KEY certificates list when enable local database user authentication if require specific certificate.

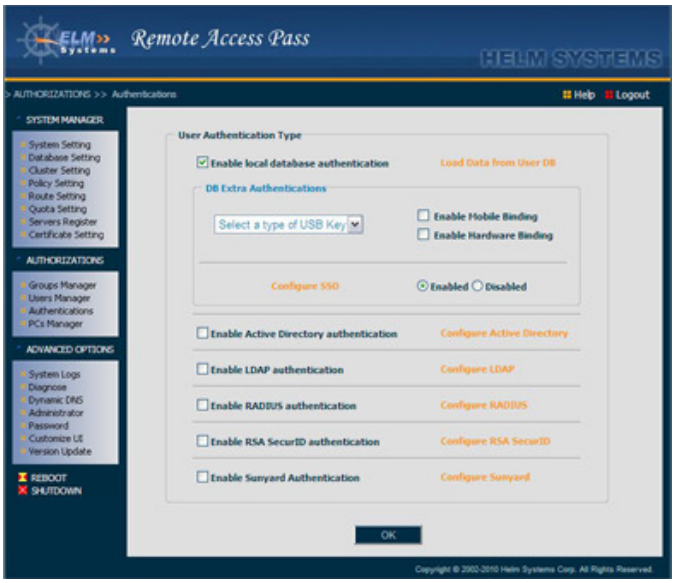


Figure 32: Extra Authentication Types List

4.3.1 Pre-load User Data from a Text File to DB (Provisioning)

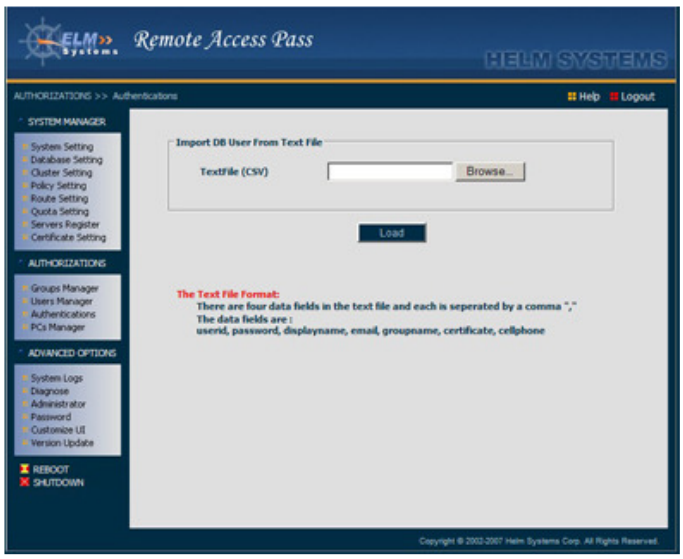


Figure 33: Import User Data from a Text File to DB

4.3.2 MS Active Directory Authentication and Pre-load User Data

Input the URL of the page of the changing user password of the AD server to make user can change their password in AD server through RAP directly.
When load the user data from AD server to local DB, the user authentication type can be assigned depend on the different cases.

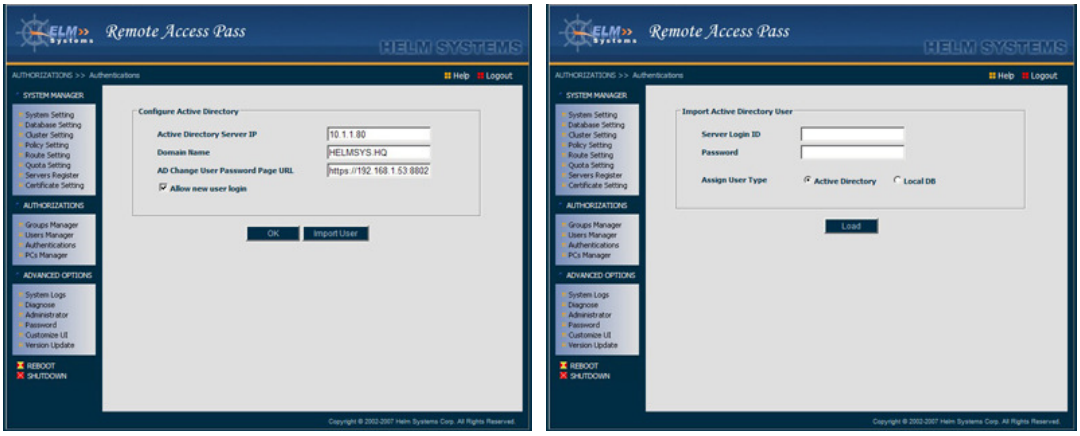


Figure 34: MS Active Directory Authentication

4.3.3 LDAP Authentication and Pre-load User Data

Input the URL of the page of the changing user password of the LDAP server to make user can change their password in LDAP server through RAP directly.
When load the user data from LDAP server to local DB, the user authentication type can be assigned depend on the different cases.

- When require extra authentication of the certificate both stored in LDAP server and USB Key, It needs to add a attribute in sysconfig.xml file located in /usr/apps/tomcat/data/.
- Make local DB authentication enable and select a USB Key supported.
- The format of attribute in sysconfig.xml is <LDAP CERT_FILED="field name of certificate stored in LDAP" /> to enable this feature, and restart system.

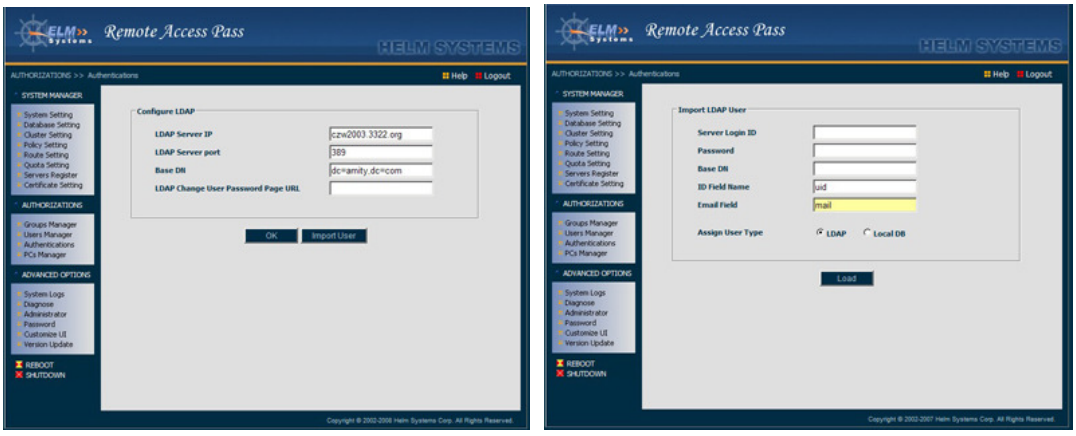


Figure 35: LDAP Authentication and Pre-load User Data

4.3.4 RADIUS Authentication

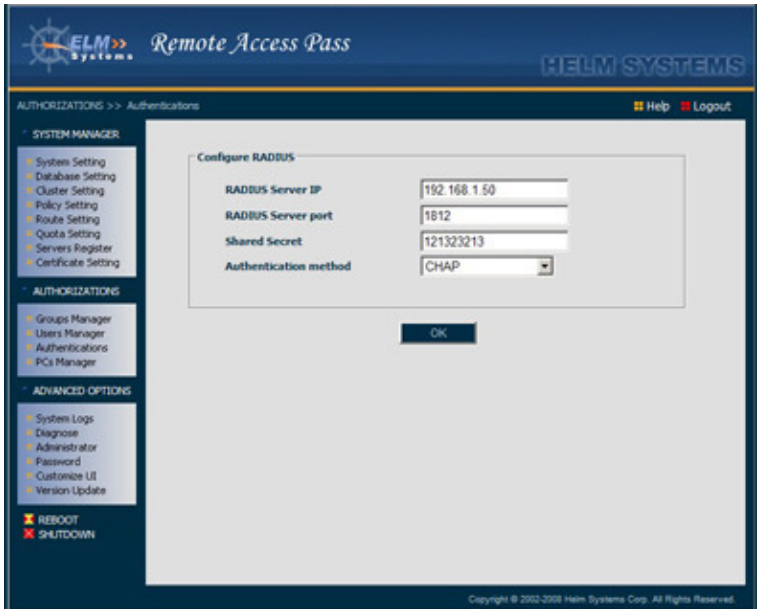


Figure 36: RADIUS Authentication

4.3.5 RSA SecurID Dynamic Token Authentication

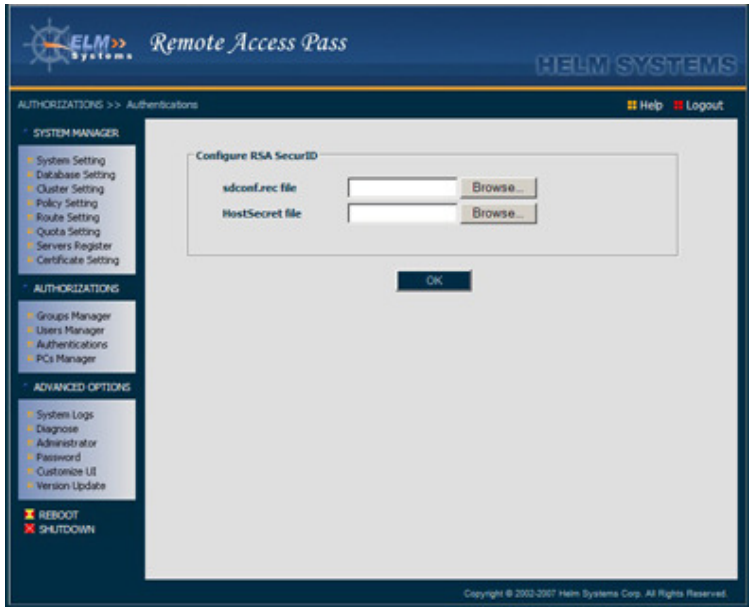


Figure 37: RSA SecurID Authentication

4.3.6 USB Key Authentication

Download and install the USB Key driver from the world images of home page of RAP

- Register a user required USB Key authentication
  - Select a kind of USB key in the keys list and click "OK" to set USB Key extra authentication flag
  - When adds a user, plug the key built in CA in the USB port
  - Click "Upload Certificate" button to upload the certificate to the DB from key
  - When there is no any certificate in this key, click "Update" button can generate a certificate both in this USB Key and in DB

- User required USB Key authentication Login to application
  - Plugs the USB Key in the USB port of the remote PC, before logins to RAP
  - Display second authentication page after you login the normal authentication first page of RAP successfully
  - Input the Key pass to start authenticating

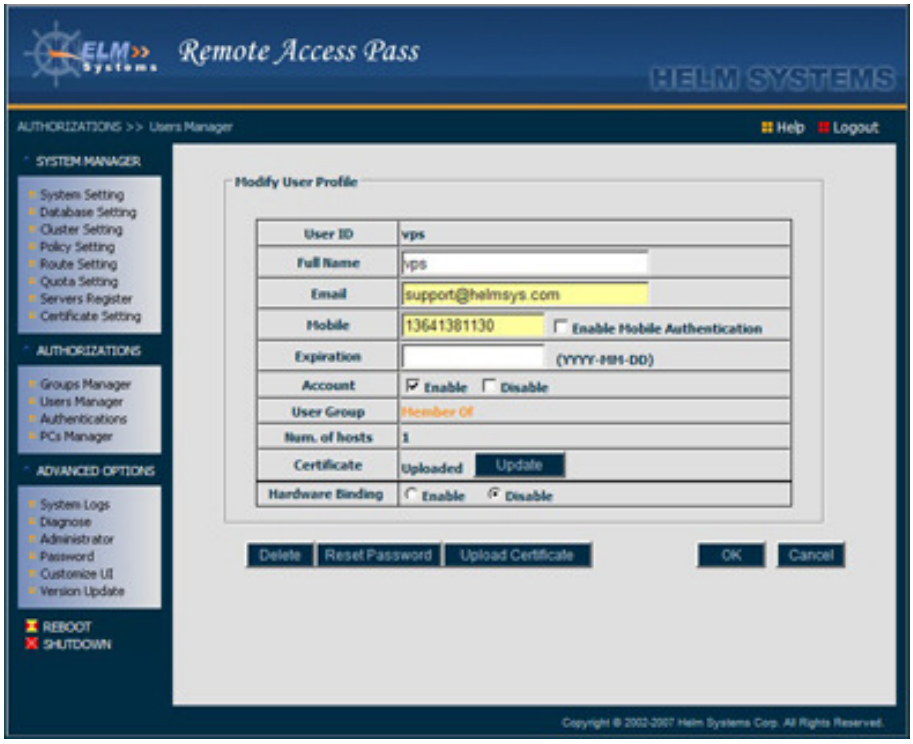


Figure 38: USB Key Authentication Registration

4.3.7 Mobile Authentication

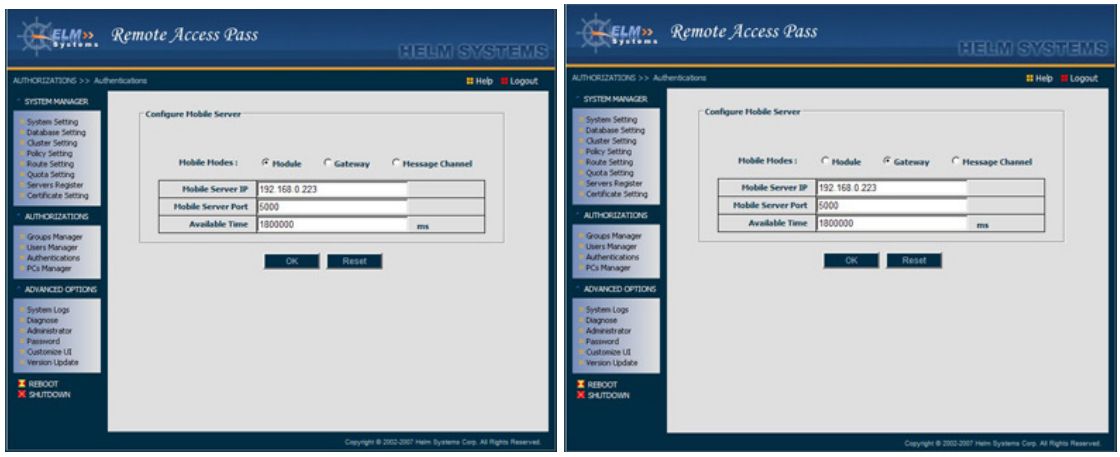


Figure 39: Mobile Module and Gateway Modes Setting

There are three mobile modes can be used:

- Module Mode: Connect a mobile hardware module device to RS232 port of RAP appliance or the RS232 port of any Windows PC in the same LAN with RAP. Plug the SIM card to this hardware module device.
- Gateway Mode: The mobile telecom gateway is installed in the corporate LAN.

There are same parameters can be input above two modes:

The IP address and port of module device or gateway

The available time (millisecond)

- Message Channel Mode: The message service center is provided by mobile provider in the Internet. The service needs authentication

Click OK: Resets the parameters of mobile server

Click Reset: Display the current data of mobile server

Figure 40: Mobile Message Channel Mode Setting

The different country may need different mobile code depend on different mobile service provider. The code should be written in the mobile.properties file.

4.3.8 Hardware bound

After select “Enable Hardware Binding”, requires the user must authenticate both userID/Password and the PC pointed by system when the user login.

Figure 41: Hardware Bound Setting

- Select the Hardware Binding in User Profile.
- The user login RAP through the PC that want to be bound , Download the plug-in package of USBKEY when user access the first login page since “Enable Hardware Binding” is selected.
- The admin views the hardware ID and confirmed the ID as a bound ID with user. Select the hardware ID from “Required Hardware ID” and click “Bind →” to see the hardware ID moved from “Required Hardware ID” to “ Bound Hardware ID”. The “Bind” finished when clicks “OK”.
- The admin select the hardware ID from “Bound Hardware ID” and click “←Remove” to see the hardware ID moved from “Bound Hardware ID” to “Required Hardware ID”. The “Unbind” finished when clicks “OK”.
- The all hardware Ids in the “Required Hardware ID” are cleared if the hardware ID in “Required Hardware ID” had not been bound by admin until three days.

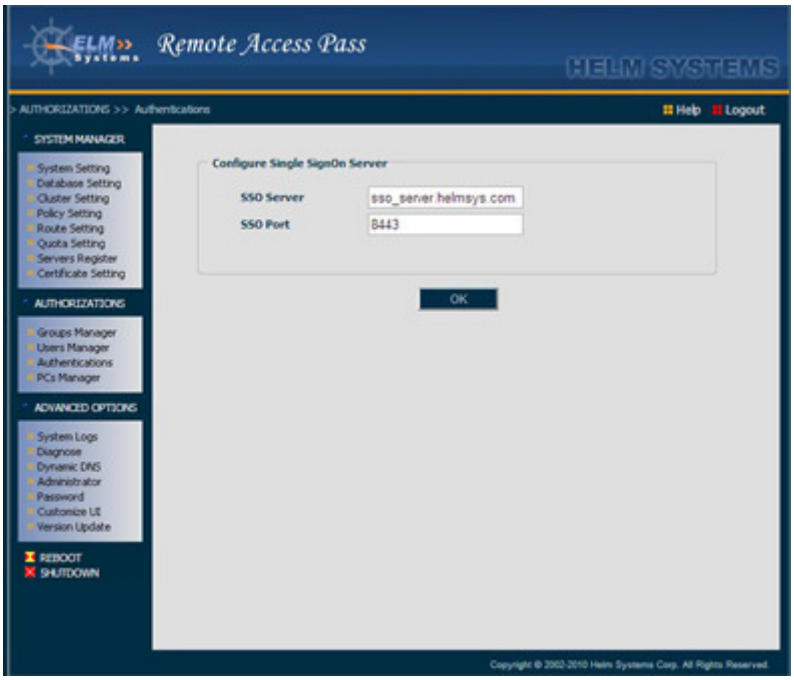


Figure 42: Single SignOn Server Configuration

4.3.9 Single SignOn Server

- Check the radio check box to enable or disable Single SignOn service on the authentication type list page. This function is corresponding to local DB authentication. It can control the target applications accessed through RAP centralize authentication and authorization..
- When the SSO service is enabled, you must configure the SSO server name first (Do not set IP address instead of server name).
  This function is powered by JASIG CAS SSO. Please access the web site" http://www.ja-sig.org" to get the detail for client application configuration.

4.3.10 Custom Authentications

- Through the API of the custom authentication system combined with RAP, define the attribute <CUSTOM NAME="", SERVER="", PORT="", SHARED_SECRET=""/> in sysconfig.xml file.
- The SUNYARD and EKEY of customed authentications (Token Ring) had been supported.
- The IP, Port and Shared Secret can be modified through following page.

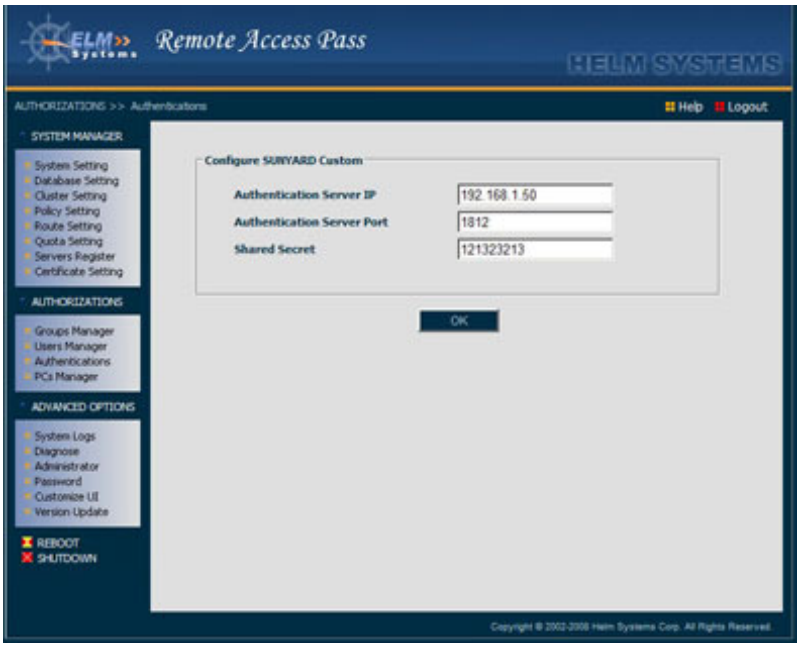


Figure 43: Custom Authentication Setting

4.3.11 Synchronization of User for Certificate stored in LDAP with Two-way SSL Authentication

Add the tag <SYNC_LDAP_USER>true</SYNC_LDAP_USER>; at the same time set tag<AUTO_ADD_USER>true</AUTO_ADD_USER> in the sysconfig.xml file to enable the synchronization of user date from LDAP to VPN after authentication.

Add the tag<GROUP_FIELD>”group name”</GROUP_FIELD> to define group name from LDAP group field name

4.4 PCs Manager

The core technology of Remote control PC is based on open source code VNC. After modified and optimized the VNC code, the management function of PC registered is added.

- The PC registration is done by user.
- From the Targets tab, target computer usage profiles can be viewed and deleted. ID numbers are assigned at the time of target computer registration.
- The Description column target computer names.
- Deletion of an owners target computer will remove the registered computer from the system and does not simply delete the log files. To delete the computer from the system, check the box to the left of the undesired profile and select the Delete link at the bottom of the checkbox column.
- The **Target Computer Profile** may be viewed by selecting the link in the Description column.
- **Owner ID** is the User ID login.
- **Owner Name** is the First and Last name fields. Users may change their registered names from the User Profile link on the Main Page screen.
- **Description** is the target computer name. Users may change the registered name of their computer using the Operations Profile link on the Main Page screen
- **Last modified on** is the date the target profile was last changed.
- **User Access Logs** may be viewed by selecting the link in the Owner column on the Targets tab. This provides specific usage data, such as login and computer access dates and times. User Access Logs may not be modified.

Figure 44: Target Computer Manager

Figure 45: View Target PC Profile

Figure 46: View User Access Log

5. Advanced Options

5.1 System Logs (View or Download)

Select the "System Logs" link

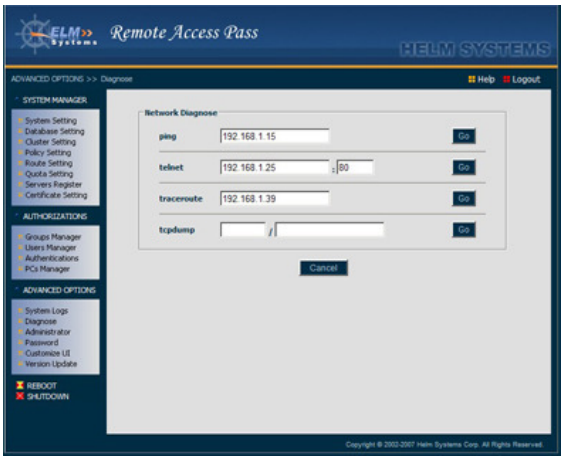
Access is gained to the log files. All error and users access messages generated by the RAP server are recorded within three files:

user_access_log.DATE.txt, localhost_access_log.DATE.txt, or catalina.out. You may view the log files within the browser by simply selecting the link to view the file or you may download it for local viewing.

Figure 47: System Log Files

5.2 Diagnose

Select the "Diagnose" link



The format of both traceroute and tcpdump are defined in

http://www.freesoft.org/CIE/Topics/54.htm

http://www.freesoft.org/CIE/Topics/55.htm

Figure 48: Status of Internal Server Connection Diagnose

5.3 Dynamic Domain Name System (DDNS)

Select the "Dynamic DNS" link

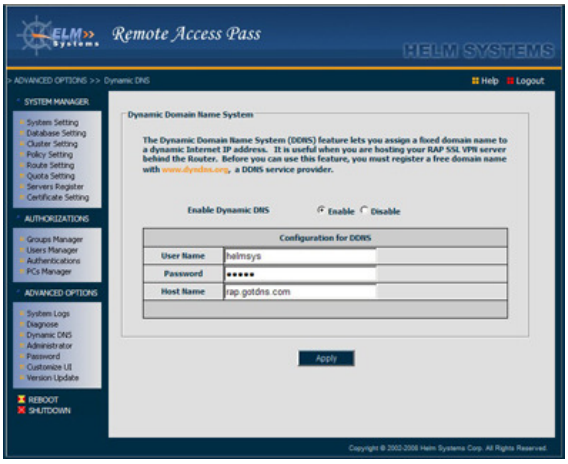


Figure 49: Dynamic DNS

The feature lets you assign a fixed domain name to a dynamic Internet IP address. It is useful when you are hosting your RAP server behind the Router. Before you can use this feature, you must register a free domain name with **www.dyndns.org**, which is a DDNS service provider.

Enable the DDNS feature

- Enter the user name (registered account name of dyndns)
- Enter the password (registered account password of dyndns)
- Enter the host name (assigned alias of dynamic DNS host in dyndns account)

5.4 Administrator

Select the "Administrator" link.

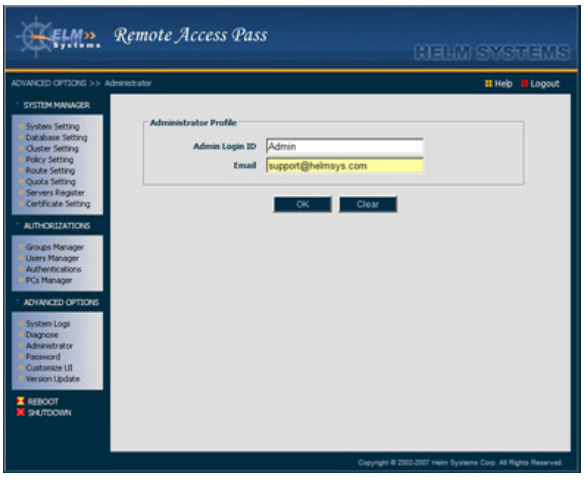


Figure 50: System Administrative Configuration

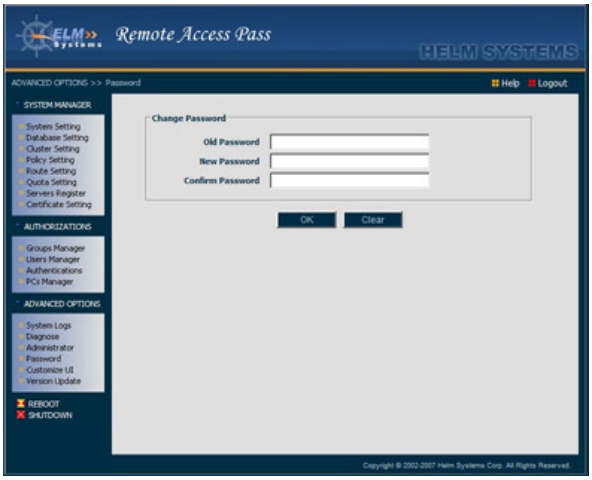
The Web Management Port may be set to a specific port for reduced visibility to casual visitors.

The Trusted IP and the Trusted Mask are set to restrict requests to a specific domain or a specific workstation. For example, setting the trusted IP to 10.8.105.20 and the network mask to the setting 255.255.255.0, permits only the workstations with IP addresses in 10.8.105.0 subnet to access this administration console.

The e-mail address set on this page is the default e-mail for system administrator event notification. This e-mail address is also provided to the end-users for technical support and for reporting system problems.

5.5 Password

Select the "Password" link

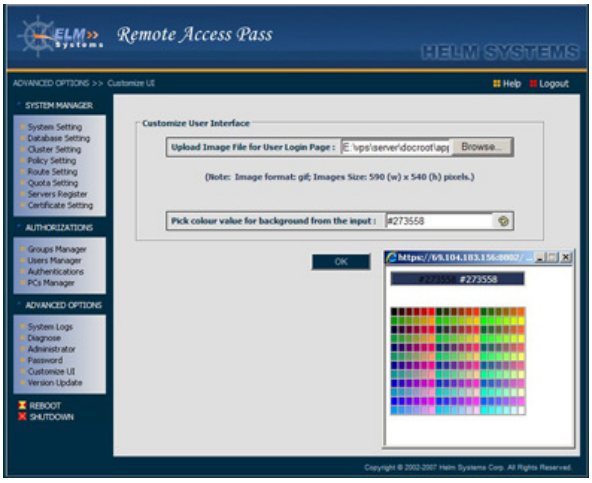


Display the text field allow admin to change his (her) password for admin console login

Figure 51: Change Admin Password

5.6 Customize UI

Select the "Customize UI" link



- Some user wants to customize the logo and background of application login page they hoped.
- The can design their own image following the request: The image size: 590 (w) x 540 (h) pixels and image format: gif.

The new image file replaces the original image of login page.
The background color of the login page can be changes either using the color picker.

Figure 52: Customize the User Interface

5.7 Version Update and Data Backup

When the system latest version is available, the provider or agent will provide it to the customer.

The administrator can update the RAP server through this tool page.

- Click "Save Current Version" button, the system can download the current version package from Helm service center to your local PC.
- Select this update package using file browser and click "Update" button, the RAP can update automatically.
- If there is any question after update the latest version, click the" Recover Pre-version" button can recover the system back to previous version.
- Click "Backup Database" button, the system can backup the data of all the tables in database to a specific file.
- Select the file that backup the data of database using file browser and click "Restore Database" button can restore the data from the file to database.

Figure 53: Update Version and Data Backup

6. Help

- Click "Help" and select "Remote Access Pass Administrator Manual", the browser will display the content of the file in right frame.
- If can't display this file, then there is no "Acrobat Reader" be installed in your PC. You can read this file after you click "Acrobat Reader" link to install it.

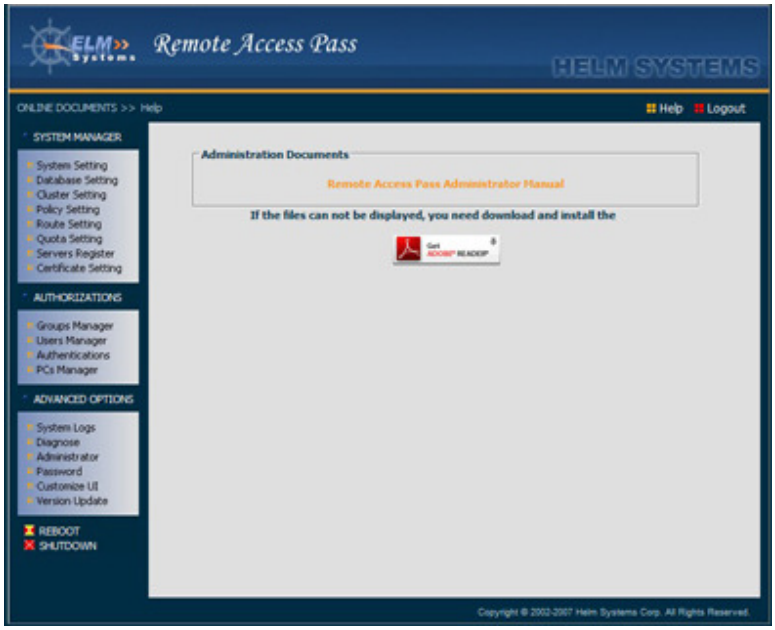


Figure 54: Online Document

7. Logout

Click "Logout" to exit the RAP admin console

8. Reboot

Click "Reboot" to restart the RAP systems

9. Shutdown

Click "Shutdown" to halt the RAP systems. After the LCD's are off except power after click "Shutdown" a couple of minutes, turn the RAP switch off.

Note: When click "Shutdown" button, the system can not be accessed remotely any more. It needs manually to restart.

Appendix (A) RAP Connections in Networks:

The firewall needs open 443# port to allow user accessing the application page of RAP.
For making the remote accessing more efficiently, all non web based applications are relay through 80# port. The firewall needs open 80# port too as well as makes http protocol detector off for 80# port.

A1. One router, one firewall with one C class

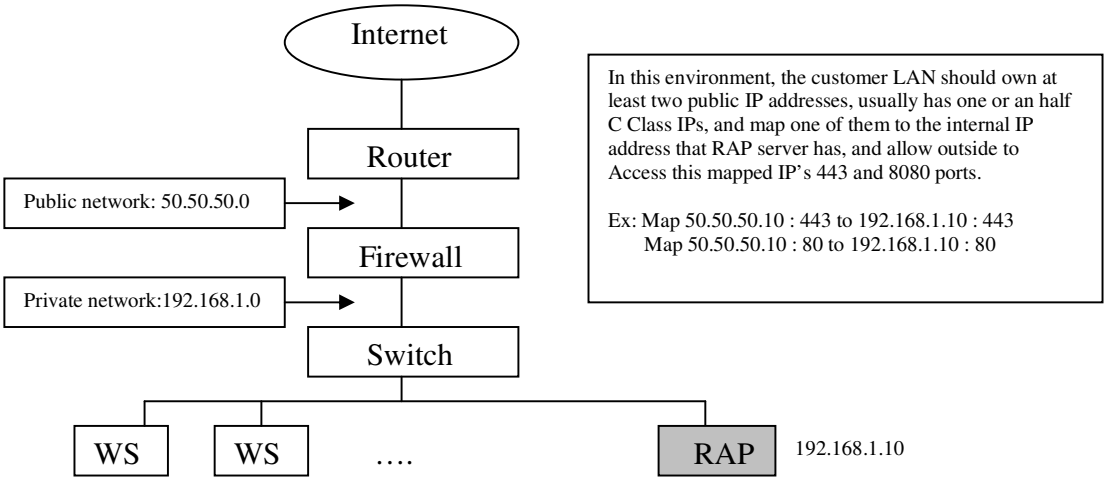


Figure A1

A2. One router with one C class

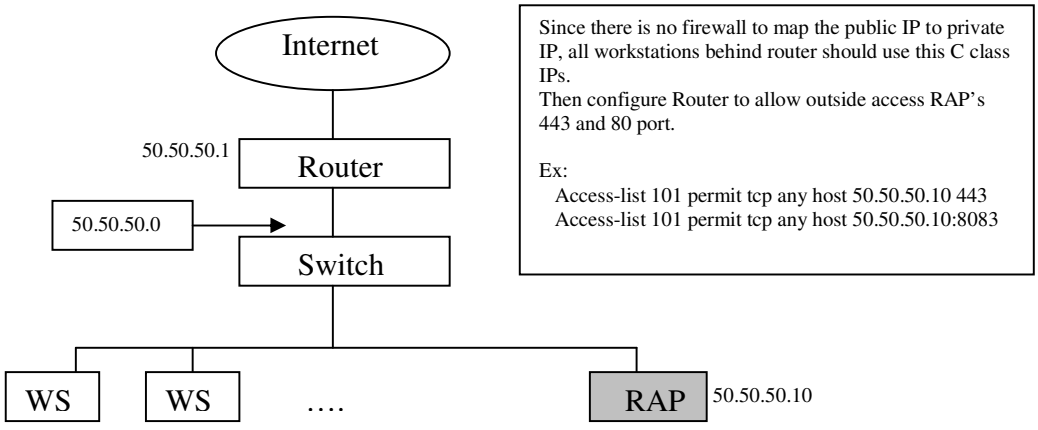
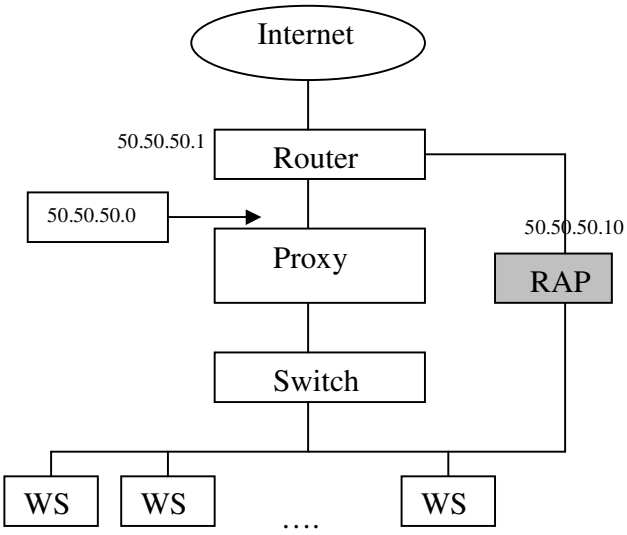


Figure A2

A3. One router, one proxy and one C class



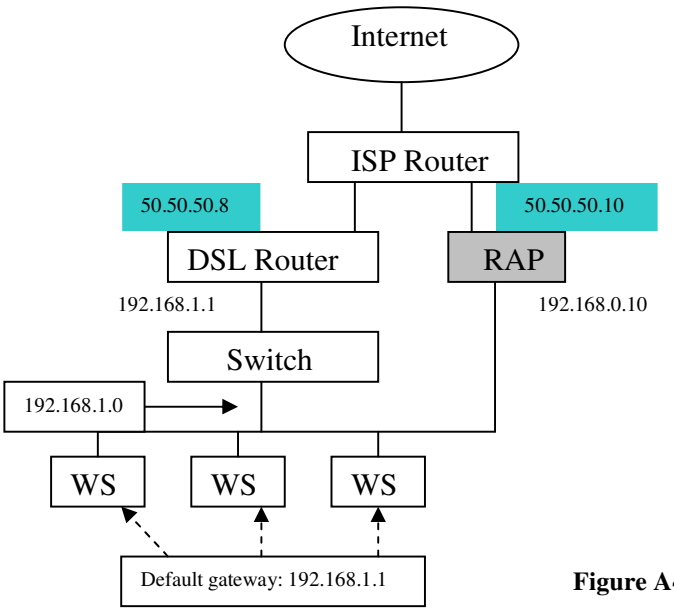
Since there is no firewall to map the public IP to private IP, all workstations behind router should use this C class IPs.
Then configure Router to allow outside access RAP's 443 and 80 port.

Ex:
Access-list 101 permit tcp any host 50.50.50.10 443
Access-list 101 permit tcp any host 50.50.50.10:80

Figure A3

A4. One DSL router, one firewall and Cable modem or DSL connection

The customers should make sure they have at least 3 IP addresses. So router, firewall and RAP can have one respectively. The physical connection is same as figure 1.
Or, there is no firewall in its environment, the customer only need to own two addresses of IP; one is for router and the other one for RAP. See figure 4.



In this scenario, RAP server uses its two Ethernet cards to connect to external and internal network. Linux firewall must be installed on RAP server, and allow http/https access coming in.

Figure A4

It needs to enable NAT and add the policy of routing in "Route Manager" of admin

A5. The customer only has a PC connecting to DSL or Cable modem

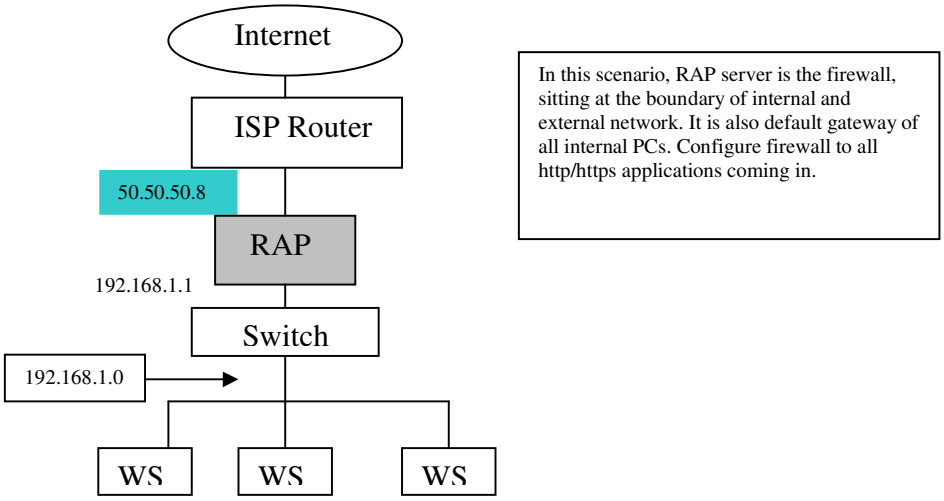


Figure A5

Notes:

- The RAP can support the case that there is a proxy in front of remote PC even this proxy needs authentication.
- The firewall or router needs mapping the 443# port to the internal IP of RAP
- RAP can be deployed to the DMZ area
- The firewall isolates all the ports except 443# and 80#

Appendix (B) Configuration of system file – sysconfig.xml:

The sysconfig.xml file is located in /usr/apps/tomcat/data/ folder in the RAP box. Following is an original template sample:

```
<?xml version="1.0" encoding="UTF-8"?>
<SysConfig>
        <APPLICATION_PORT>8805</APPLICATION_PORT>
        <TUNNEL_PORT>443</TUNNEL_PORT>
        <SYSTEM_INITIALIZED>Y</SYSTEM_INITIALIZED>
        <SYS_ADMIN_PASSWORD></SYS_ADMIN_PASSWORD>
        <ADMIN_MASK>0.0.0.0</ADMIN_MASK>
        <AUTO_ADD_USER></AUTO_ADD_USER>
        <MAIL_USER></MAIL_USER>
        <ENABLE_DB_LOG>Y</ENABLE_DB_LOG>
        <DATABASE_TYPE>HSQL</DATABASE_TYPE>
        <SSO_SERVER>192.168.1.62</SSO_SERVER>
        <DNS_SERVER></DNS_SERVER>
        <ADMIN_IP>127.0.0.1</ADMIN_IP>
        <SERVER_NAME> </SERVER_NAME>
        <ROW_PER_PAGE>10</ROW_PER_PAGE>
        <ALLOW_TUNNEL>1</ALLOW_TUNNEL>
        <LICENSE_CODE></LICENSE_CODE>
        <SSO_PORT>8443</SSO_PORT>
        <RELAY_PORT>80</RELAY_PORT>
        <SERIAL_ID></SERIAL_ID>
        <LICENSE_MODE>CONCURRENT_USER_MODE</LICENSE_MODE>
        <FIX_IP></FIX_IP>
        <ENABLE_SSO>1</ENABLE_SSO>
        <AUTODISCOVER_SERVER></AUTODISCOVER_SERVER>
        <CRL></CRL>
        <DEBUG_SCHEME></DEBUG_SCHEME>
        <MAIL_PWD></MAIL_PWD>
        <MAIL_SERVER></MAIL_SERVER>
        <SYS_ADMIN_NAME>Admin</SYS_ADMIN_NAME>
        <CLIENT_AUTH>false</CLIENT_AUTH>
        <TUNNEL_PROTOCOL>https</TUNNEL_PROTOCOL>
        <VPS_PORT>8088</VPS_PORT>
        <LOOK_FEEL>0</LOOK_FEEL>
        <EXTERNAL_CRYPTO_ALG>Y</EXTERNAL_CRYPTO_ALG>
        <CUSTOMER_CRYPTO_KEY>12345678</CUSTOMER_CRYPTO_KEY>
        <SYSLOG_SERVER></SYSLOG_SERVER>
        <RDP_PORT>8803</RDP_PORT>
        <SYS_ADM_EMAIL>support@helmsys.com</SYS_ADM_EMAIL>
        <SYSLOG_PORT></SYSLOG_PORT>
        <PROXY_PORT>8804</PROXY_PORT>
        <DEFAULT_NETWORK_INTERFACE>eth0</DEFAULT_NETWORK_INTERFACE>
        <DEFAULT_GATEWAY></DEFAULT_GATEWAY>
        <ADMIN_PORT>8802</ADMIN_PORT>
        <SYNC_LDAP_USER>false</SYNC_LDAP_USER>
        <SUPPORTED_SERVER>
                <WWW NAME="Web Server"/>
                <EXCHANGE NAME="Exchange Server"/>
                <CLIENT_SERVER NAME="Restricted Client/Server"/>
                <GENERIC_CS NAME="Generic Client/Server"/>
                <VPN NAME="Network Tunneling"/>
                <TELNET NAME="Telnet Service"/>
                <SSH NAME="SSH Service"/>
                <FTP NAME="FTP Service"/>
                <TERMINAL_SERVER NAME="Terminal Service"/>
                <POP3 NAME="POP3 Server"/>
```

```
            <IMAP NAME="IMAP Server"/>
        </SUPPORTED_SERVER>
        <SUPPORTED_AUTH>
            <CEBC DESCRIPTION="CapInfo USB Key" TYPE="USB_KEY"/>
            <HAIKEY_1000 DESCRIPTION="HaiTai USB Key" TYPE="USB_KEY"/>
        </SUPPORTED_AUTH>
        <NETWORK_INTERFACES>
            <eth0 DEFAULT_GATEWAY="192.168.1.1" ENABLE_NAT="false" IP="192.168.1.62"
SUBNET_MASK="255.255.255.0"/>
        </NETWORK_INTERFACES>
        <REMOTE_RAPS/>
        <AUTHENTICATION>
            <DB ENABLED="true"/>
            <LDAP ADMIN_NAME="" BASE_DN="" CERT_FIELD="" ENABLED="false" GROUP_FIELD=""
ID_FIELD="" MAIL_FIELD="" PASSWORD="" PORT="389" SERVER=""/>
            <RADIUS AUTHENTICATION_METHOD="" ENABLED="false" PORT="0" SERVER=""
SHARED_SECRET=""/>
            <CUSTOM ENABLED="false" NAME=""/>
        </AUTHENTICATION>
</SysConfig>
```

You can modify any parameter in this file following its exactly name.
For example:

1. Login the administrator system of RAP: https://x.y.m.n:8802 (For security reason)
2. Uses the URL: https://x.y.m.n:8802/servlet/AdmServlet?handler=SysConfig&action=config&SysConfig.DEBUG_SCHEME=5&SysConfig.ROW_PER_PAGE=20 to replace the current URL

The x.y.m.n is the IP address of this RAP.

After runs above URL, the parameter DEBUG_SCHEME of sysconfig.xml is modified to 5. (Debugging record level change to 5) and the parameter ROW_PER_PAGE of sysconfig.xml is modify to 20. (Display 20 user lists per page in the RAP admin system.