Air Marshal

Authentication Gateway

Version 1.0

IEA Software, Inc.

Software License Agreement

By purchasing or installing Air Marshal Authentication Gateway, you indicate your acceptance of the following License Agreement.

Ownership of Software You acknowledge and agree that the computer program(s) and associated documentation contained with the Air Marshal Authentication Gateway (collectively, the "Software") are owned exclusively by IEA Software, Inc. and/or its licensors. The Software contained in the package is protected under copyright laws and all copyright and other intellectual property rights relating to the Software are and remain the exclusive property of IEA Software, Inc. and/or its licensors. You may not rent or lease the Software, but you may transfer the Software and accompanying materials on a permanent basis provided you retain no copies and the recipient agrees to the terms of this Agreement.

License IEA Software, Inc. grants to you, and you accept, a limited, non-exclusive and revocable license to use the Software. You agree to use the Software in machine-readable object code form only as authorized in this License Agreement. This License Agreement does not convey any title or interest in the Software to you. You may only use the licensed number of copies of the Software as stated in your purchase agreement.

Scope of License You may not make any changes or modifications to the Software, and you may not decompile, disassemble, or otherwise reverse engineer the Software. You may not load, rent, lease or sublicense the Software or any copy to others for any purpose. You agree to use reasonable efforts to protect the Software from unauthorized use, modifications, reproduction, distribution and publication. You are not permitted to make any uses or copies of the Software that are not specifically authorized by the terms of this License Agreement. Your adherence to this License Agreement will allow IEA Software, Inc. to continue developing innovative and useful products and providing a high level of customer service and support. If you do not comply with the terms of this License Ageement, your license will be revoked.

Updates and Support All software updates are available via the IEA Software, Inc. web site. A maintenance contract is available for major version upgrades, which is not included or covered as part of the basic purchase agreement. Technical support is available via E-Mail, support mailing lists, or a purchased telephone support contract.

Trademarks IEA Software, Inc., and the associated logo(s) are registered trademarks. All images, photographs, animations, audio, video and text incorporated into the Software is owned by IEA Software, Inc., unless otherwise noted by Trademark.

Restricted Rights The Software is provided with U.S. Governmental Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraph ©(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs ©(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19 as

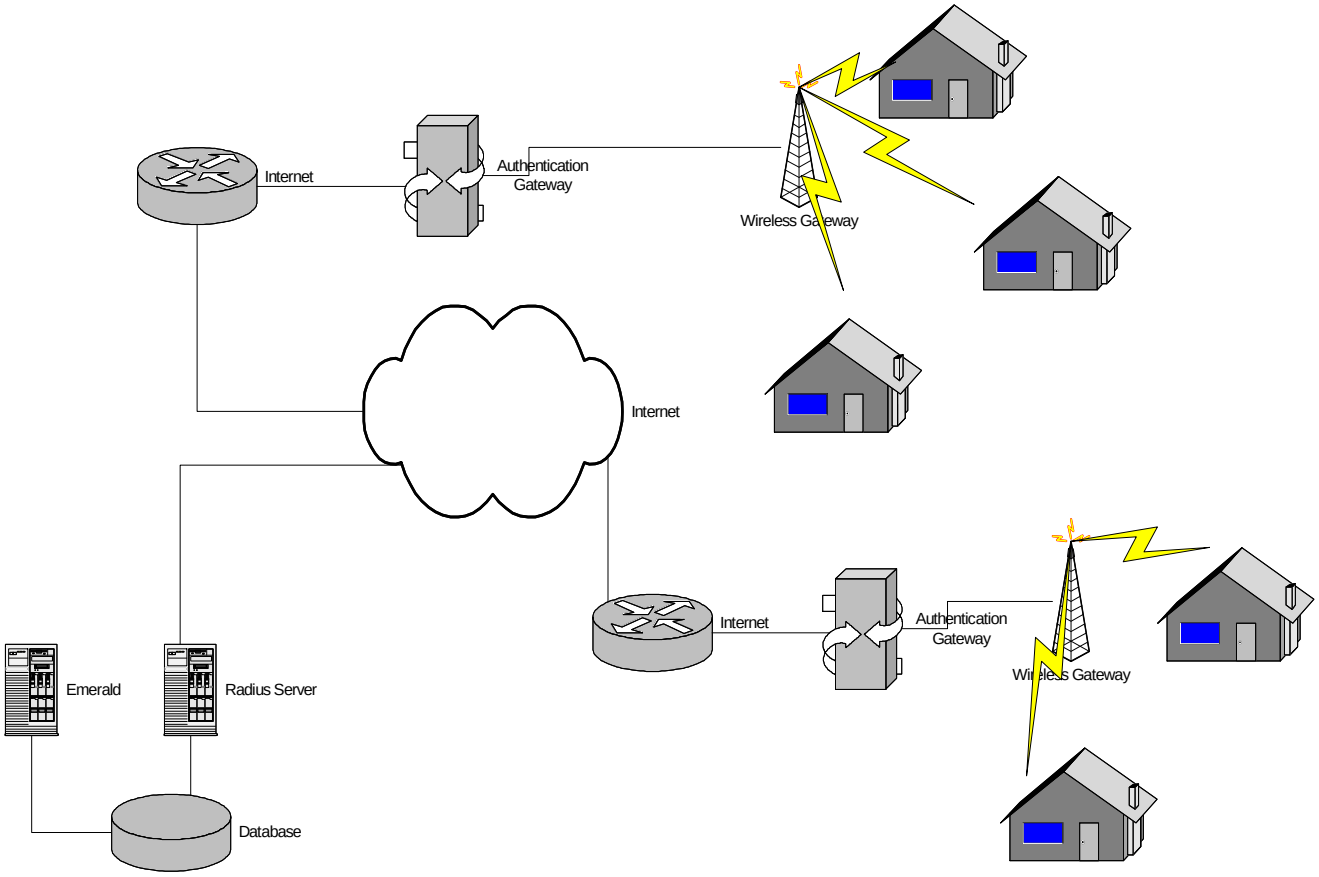
applicable. The Software is also protected by International Treaty Provisions. Manufacturer is IEA Software, Inc. PO BOX 1170 Veradale WA, 99037.

Miscellaneous This License Agreement shall be construed, interpreted and governed by the laws of the State of Washington. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, enforcement of the remaining terms shall not be affected. Failure of either party to enforce any rights or to take action against the other party in the event of any breach of this Licensing Agreement shall not be deemed a waiver of any subsequent enforcement of rights.

Limitations of Liability and Remedies In no event shall IEA Software, Inc. or its licensors be liable for any loss of profit or any other commercial damage, including but not limited to special, incidental, consequential or other damage, even if IEA Software, Inc. or its licensors are advised, in advance, or the possibility of such damages. IEA Software, Inc. and its licenser's entire liability and your exclusive remedy shall be, at IP Method's option, either (a) return of the price paid, or (b) repair or replacement of the Software. To the maximum extent permitted by applicable law, IEA Software, Inc. and its licensors disclaim all other warranties, either express or implied, including but not limited to, implied warranties with regard to the Software, the accompanying material. This Limited Warranty is void if failure of the Software has resulted from accident, abuse or misapplication. You may have other specific legal rights which vary from state/jurisdiction to state/jurisdiction.

Should you have any questions concerning this license agreement, please contact IEA Software, Inc. at PO BOX 1170 Veradale WA, 99037 U.S.A. Phone # 509.444.2455.

Table of Contents



Introduction

Authentication gateways provide an inexpensive simple way for the customer to obtain Internet access without having to install or configure software. Simply plug-in and your default home page is automatically 'captured' and redirected to the authentication gateway. After providing a login, password or signing up for new service – the user is allowed access to the rest of the network.

Authentication gateways can be used in a wide range of environments where Ethernet technology provides for client network access. Today the most popular application comes from controlling access to wireless LANs.. However authentication gateways have been around for quite some time in other settings such as hotels, cyber cafes and universities.

The authentication gateway utilizes RADIUS to authenticate clients and account for usage. This allows the gateway to take advantage of features the service provider's current authentication and billing systems provide such as controlling concurrent access, usage billing or participating in a roaming network.

Security Considerations

Authentication gateways are responsible for controlling access to the network. There is no additional security to protect the integrity or confidentiality of data moving over the Ethernet network. This is usually of little concern for Internet users where SSL or encrypted VPNs can still be used to protect confidential information. If data encryption for all traffic is required, It is recommended That You use a

Radius server that provides EAP authentication compatible with wireless access points and network access servers supporting 802.1x and RADIUS.

Note: Security features such as WEP/pre shared keys or 802.1x may be used in addition to the authentication gateway.

System requirements

Linux

- RADIUS server for client authentication and accounting.
- PERL (required for installation)
- Any distribution of Linux supporting kernel version 2.2 or higher.
- IPTables or IPChains
- X86 based CPU
- Computer must have 2 network interface cards installed.

Windows

- RADIUS server for client authentication and accounting.
- Windows 2000 (Professional or Server) or WindowsXP (Home or Pro) or Windows Server 2003.
- X86 based CPU
- Computer must have 2 network interface cards installed.

Linux Installation

Download the Air Marshal archive (airmarshalv1_linux.tar.gz) into a temporary folder.
To un-archive the file type:
gzip –d airmarshalv1_linux.tar.gz
tar –xf airmarshalv1_linux.tar

Next, run the installer:
./install.pl

Press ‘C’ followed by return.

The portal server is now installed and automatically configured to start when the system is booted. You can disable automatic startup on Linux by running the following command: chkconfig –level 345 portald off

Now start the server in debug mode:
/usr/local/portal/portald –debug

Using a web browser go to http://[addressofmyserver]:81/settings. You will either be prompted to create an admin password or asked for an existing password. If you've previously installed other IEA-Software products such as Emerald or RadiusX the password is the same password used for the admin web interface.

Next follow the instructions in the 'Server configuration' chapter for configuring the server. (Minimally Licensing, Network options and Authentication must be configured)

Click 'Save' to complete the startup of the server. If there is an error please correct it and click 'Save' again.

After testing the server works correctly you can press ctrl-c to stop the portal server in debug mode and start it as a background task. To do this type:
/usr/local/portal/portald

Windows Installation

Download the Air Marshal installation (airmarshal.exe) into a temporary folder.

Execute the program to install Air Marshal. Select the standard install and follow the instructions to install Air Marshal into the directory of your choice.

Open up a command prompt and change to the directory where you installed Air Marshal to. Start the server in debug mode using the following command:

```
portal –debug 255
```

Using a web browser go to http://[addressofmyserver]:81/settings. You will either be prompted to create an admin password or asked for an existing password. If you've previously installed other IEA-Software products such as Emerald or RadiusNT the password is the same password used for the admin web interface.

Next follow the instructions in the 'Server configuration' chapter for configuring the server. (Minimally Licensing, Network options and Authentication must be configured)

Click 'Save' to complete the startup of the server. If there is an error please correct it and click 'Save' again.

After testing the server works correctly you can press ctrl-c to stop the Air Marshal server in debug mode and start it as a background task. To do this type:

```
net start AirMarshal
```

from a command line or use the Control Panel/Administrative Tools services applet to start the Air Marshal Authentication Gateway service.

Windows Filter Driver Installation

For Windows, Air Marshal utilizes the IP Filter Driver interface to filter and redirect content. Only one filter driver may be active at any one time. Therefore, Air Marshal cannot be installed onto a Windows computer that has another application using the IP Filter Driver.

The Windows Installer will install the filter driver and configure it to auto start when you install Air Marshal. If the filter driver failed to install, you can use the below instructions to manually install it.

1. Open a command prompt and change directories to the directory you installed Air Marshal to.
2. Install the filter driver using the following command:

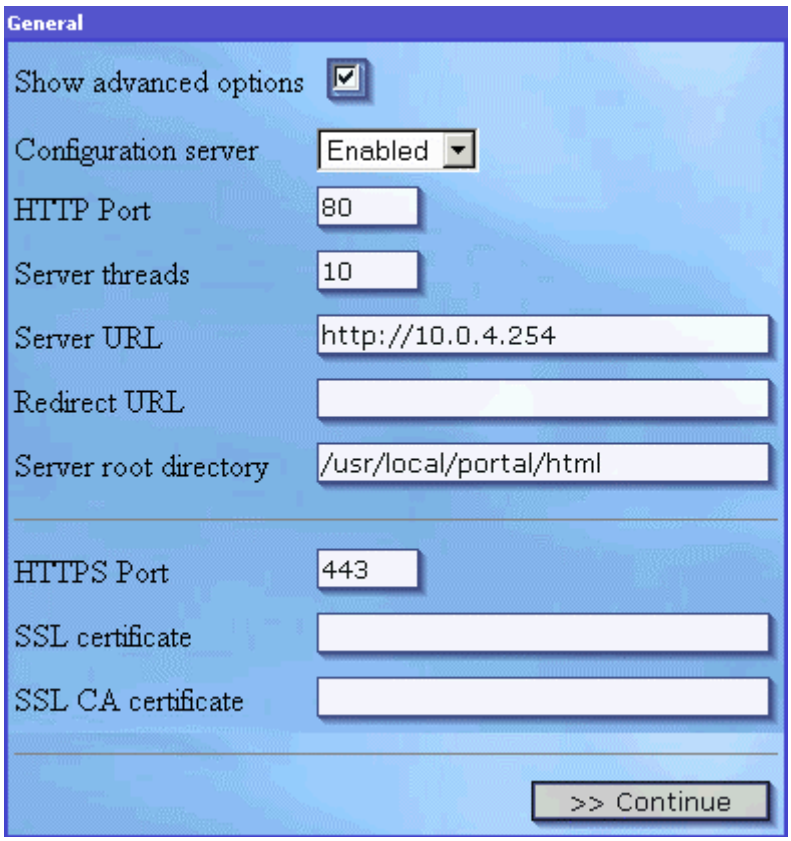
   ```
   Instdrv AirMarshalFilter "c:\program files\Air Marshal\ipfilter.sys"
   ```

3. Start the filter driver using the following command:

   Net start AirMarshalFilter

Server configuration

General

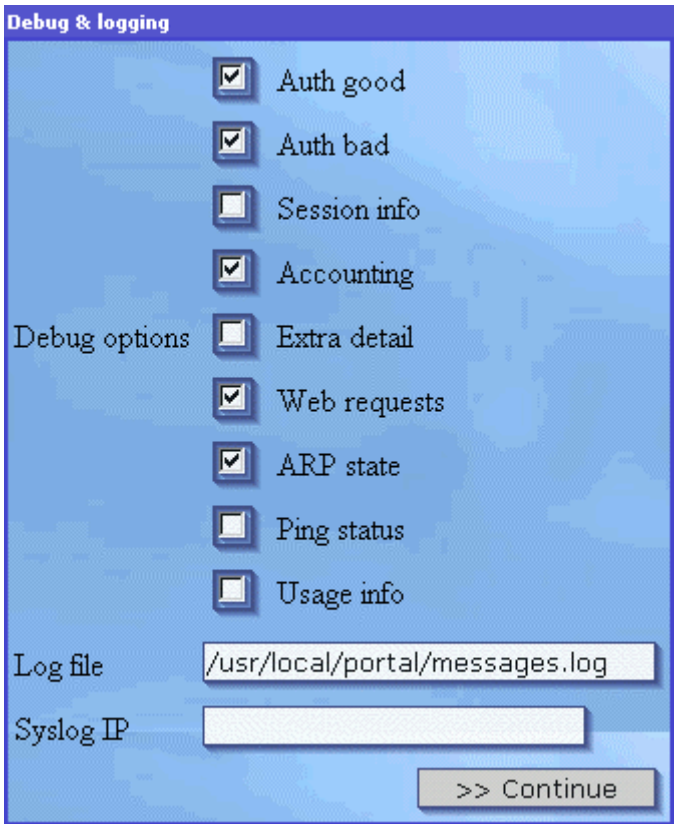


*Note: all general options except Show advanced, Server URL and Server root directory require the server to be restarted before they will take effect.

Option	Comments
Show advanced options	When checked all available options are displayed in the Air Marshal administrator. When un-checked advanced options are hidden from view. The screenshots in this document assume advanced options are enabled.
Configuration server	Controls whether or not the configuration server is accessible while the portal server is running. If this option is disabled the configuration server can be enabled when needed by starting portal server with the flag '–config'
HTTP Port	HTTP Port this server will listen for requests
Server threads	Number of concurrent web accesses the server can handle at a time. The default and suggested value is 10.
Server URL	URL of this server. For example http://10.0.4.254:81/
Redirect URL	URL users will be redirected after authenticating. If left blank the user is redirected to the page they initially intended to before being asked to login to the portal.
Server root directory	Root directory under which the html files for the authentication web interface can be found.
HTTPS Port	If using SSL this is the https port the server will listen for SSL requests.
SSL Certificate	File containing both this sites public and private keys in .pem format.
SSL CA Certificate	File containing the CA's certificate chain in .pem format. Follow your CA's documentation on obtaining this file as well as generating client certificates and issuing a CSR. The same requirements that apply to SSL on the apache web server also work for the portal server.

Debug & Logging

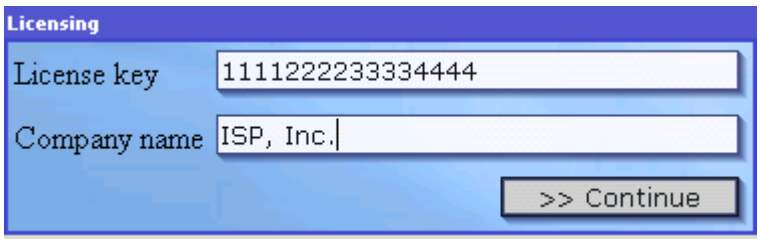
Debug options control the types server messages to be sent to a local Log file or syslog host.



*Note: Changes to 'Log file' or 'Syslog IP' require the server to be restarted before they take effect.

Option	Log Freq	Description
Auth Good	Low	Successful authentication messages
Auth Bad	Low	Unsuccessful authentication messages
Session info	Low	Details about significant changes in a users session, such as logging in or logging out.
Accounting	Low	RADIUS accounting related messages, including queue statistics.
Extra detail	High	Enables more detail about internal server functions
Web requests	Medium	Shows all web requests and the client URLs that access the portal. Authenticated user names are also displayed if available.
ARP state	High	Show ARP query statistics.
Ping status	High	If a ping script is configured this option shows weather individual ping attempts were successful.
Usage info	High	Shows information related to usage collection such as bytes and packet information as well as rule matching status info.
Log file	N/A	Filename to write the log output to
SyslogIP	N/A	IP Address of syslog server used to write logging information. All messages are sent to the local4 logging facility.

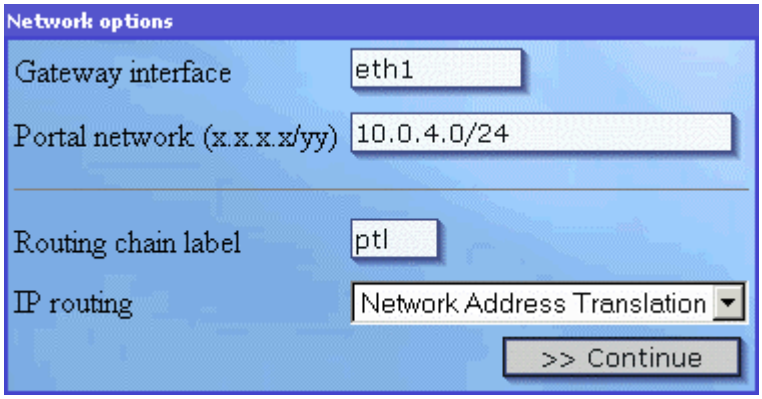
Licensing



Please contact our sales department (sales@iea-software.com) for an Air Marshal license key.

Network options

Network interfaces and subnets controlled by the authentication gateway are configured through this menu.

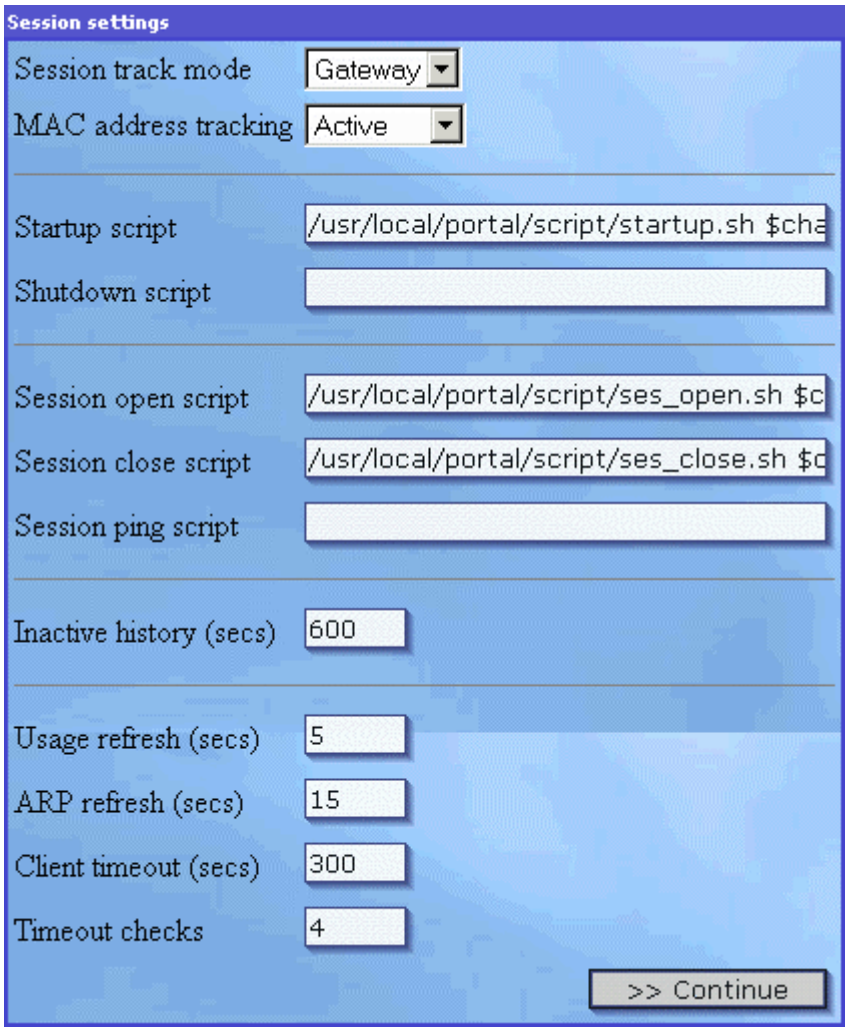


Note: The windows platform supports only 'Gateway interface'. Before selecting an interface, the network device you intend to use must be installed and enabled.

Option	Description
Gateway interface	Name of the Ethernet interface to which the user gateway network is attached. If there is more than one interfaces being used list each one delimited by a space. This option is used for the collection of ARP statistics.
Portal network	Subnet of the user gateway network. In the format (ip-address/subnet bits) There are 24 bits in a class C network.
Routing chain label	All firewall rules managed by the portal server are configured with a label specified to distinguish portal managed rules from others in the system. Note: this field is four characters long.
IP routing	Routing mode, either Static or NAT. Static assumes the network is being routed. NAT enables the Linux IP Masquerading feature on the user gateway network.

Session settings

Options controlling what actions to take to configure network access for clients as they logon or off as well as how to determine the status of a clients connection during the course of their session are configured through this menu.



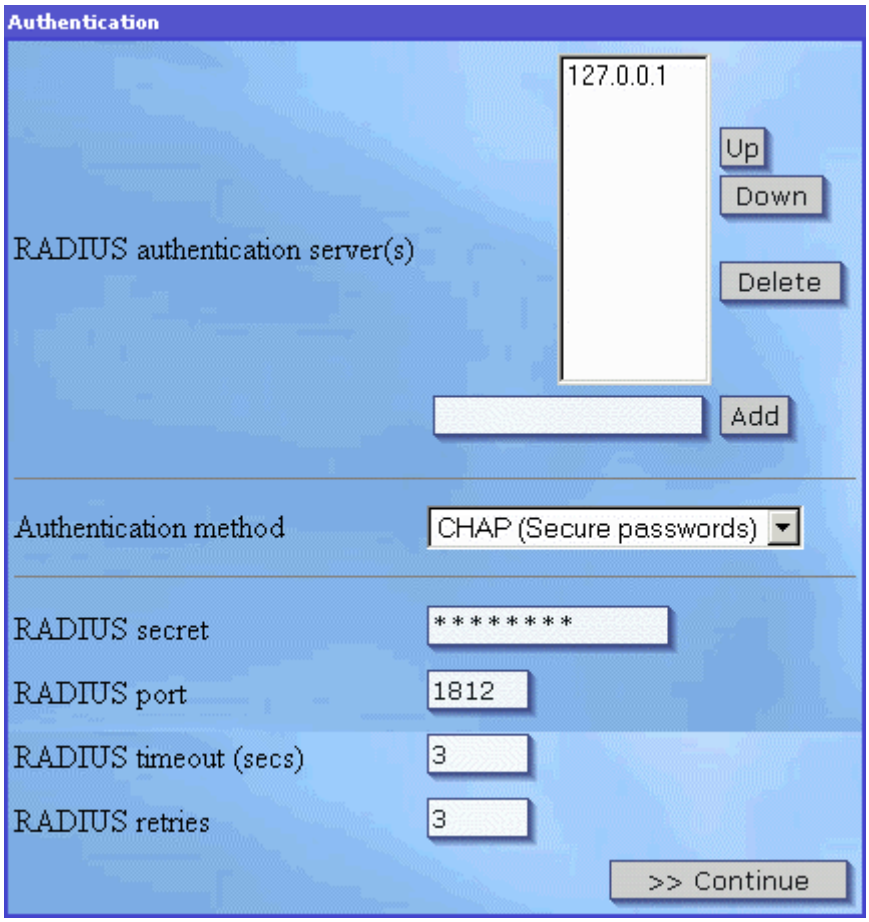
See 'Customizing' for more information on configuring scripts.
Note: Scripts are not used by default for the Windows version of Air Marshal. However they can be added to support custom actions as users login or logout.

Option	Description
Session track mode	Gateway or Routed. Gateway mode is recommended and assumes all clients are connecting through the same physical network. This mode allows the collection of client MAC information. Routed mode assumes all clients are being accessing the network through a secondary router. If there are a mix of

	directly connected and routed users on the network – select the 'Gateway' mode. If routed mode is enabled a 'Session ping script' is required to test reachability of clients.
MAC address tracking	Setting this option to 'Active' or 'Passive' prevents others from using the sessions of another by setting or having been incorrectly assigned the same IP address. Active performs ARP queries at normal intervals while Passive does not. This allows quicker detection of disconnected clients. The default and recommended setting is 'Active'.
Startup script	Run when the portal server starts up. Configures initial routing rules
Shutdown script	Run when the portal server shuts down.
Session open script	Configures all rules necessary for client to access the network after having successfully authenticated.
Session close script	Configures all rules necessary to revoke this client's access to the network after the their session has been closed.
Session ping script	Pings a client to see if they are still connected to the network. Script returns 0 if ping was successful. Any other return code indicates the client could not be contacted. Its recommended ping scripts not be used if 'Session track mode' is configured for gateway and all clients are connected to the same physical network.
Inactive history	The length of time inactive sessions should be kept in the "Who's Online" list after becoming inactive.
Usage refresh	Interval usage statistics when all open sessions will be updated.
ARP refresh	Interval when a sessions ARP info is rechecked.
Client timeout	Length of time a session can remain open without receiving a positive ARP or Ping response from the client.
Timeout checks	Number of ping attempts over the client timeout interval.

Authentication

As clients login their authenticated and authorized by the RADIUS server. This menu provides the necessary server contact information.

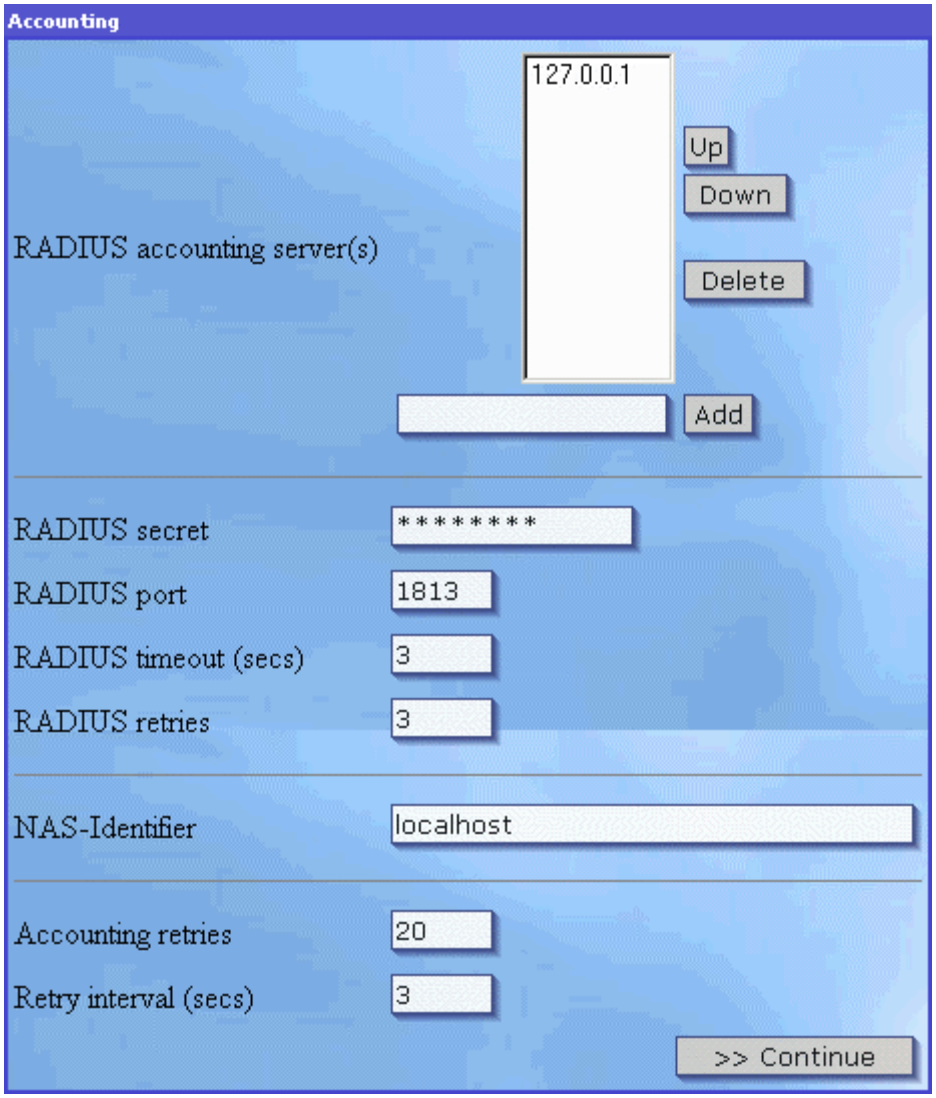


Option	Description
RADIUS authentication server	IP address/hostname of RADIUS authentication server. If Multiple servers are entered they are contacted in the order they appear if there was no response from the previous server. Note: currently all defined authentication servers share the same port and secret settings.
Authentication method	CHAP or PAP. CHAP protects the user's password entered in the web form by sending it in an encrypted form over the network -- however some RADIUS servers may not be able to support it. If this is the case switching to PAP will send passwords in clear text over the network. If it is possible for others to intercept network traffic between the gateway and client it is recommended SSL be enabled if PAP is used.
RADIUS secret	RADIUS shared secret. This secret must match the secret configured in the RADIUS server for the auth gateway.
RADIUS port	RADIUS authentication UDP port. Traditionally 1645, officially 1812.
RADIUS timeout	Length of time to wait for a response to an authentication request before giving up.

RADIUS retries	Number of authentication timeouts allowed before giving up on the authentication and returning a timeout error to the client. Also used in determining weather an authentication server is available.

Accounting

As clients logon and off accounting records containing a timestamp, identifying and usage data are logged to the RADIUS server. This menu provides the necessary server contact information.



Option	Description
RADIUS accounting server	IP address/hostname of RADIUS accounting server. If Multiple servers are entered they are contacted in the order they appear if there was no response from the previous server. Note: currently all defined authentication servers share the same port and secret settings.
RADIUS secret	RADIUS shared secret. This secret must match the secret

	configured in the RADIUS server for the portal.
RADIUS port	RADIUS accounting UDP port. Traditionally 1646, officially 1813.
RADIUS timeout	Length of time to wait for a response to an accounting request before giving up.
RADIUS retries	Number of accounting timeouts allowed before trying the next available accounting server.
NAS-Identifier	IP Address or hostname of this server, if a hostname is entered it is recommended to be resolvable via DNS.
Accounting retries	Total number of attempts to deliver an accounting message before discarding it.
Retry interval	Base retry interval for previous failed accounting attempts. Note: the retry interval automatically increases after the first failed accounting attempt. This allows for longer periods where an accounting server is not available.

Customizing

The core portal server communicates with the user and server operating system through a configurable set of html files and external programs. Files included with the server provide general functionality that can be used as a template for creating a customized user interface and unique services for clients.

HTML

The files in the table below make up the user interface. The portal server sends each file to the user where appropriate. You cannot link to or directly reference files on the portal server outside of .gif, .jpg, .js or .ptl (html) in the portal html directory. See the variable listing below for a list of available variables.

HTML file	Description
ack.html	Displayed after a successful login. Indicates the user logged in and displays information about the session.
nak.html	Displayed after an unsuccessful login. Usually shows a message to try again and redisplays the login page.
login.html	Main login page
logout.html	Displayed after the users session has closed
error.html	Displayed in place of one of the other html files. Indicates a system error that is not normal, for example a missing html file or internal error.
status.html	After successfully logging in this displays information about the users session, how much time they've used so far, time remaining…etc.

Session scripts

The types of session scripts in the table below are provided with the server. See 'Session settings' for more information on configuring scripts and parameter passing. A server shutdown and ping script can also be defined – although they are not provided with the server. See the variable listing below for a list of available variables.

Script	Description
startup.sh	Runs when portal starts up to configure initial firewalling rules for the gateway network. Note: If the startup script does not return 0, the portal server will not start.
ses_open.sh	Runs after a user successfully authenticates to provide network services to the user. If this script does not return 0, the users session will not start.
ses_close.sh	Runs after a users session has closed. If this script does not return 0, the session shall be considered closed from an accounting point of view – whether service was actually terminated or not. Sessions that do not close successfully are marked as errors and appear with a red background in the "who's online" display.

On the Linux platform, use these references to help customize the server startup/shutdown and session start/stop scripts.

IPTables tutorial (Configures filtering, NAT and forwarding rules)
[http://iptables-tutorial.frozentux.net/iptables-tutorial.html]

IPChains howto (Configures filtering, NAT and forwarding rules)
[http://www.tldp.org/HOWTO/IPCHAINS-HOWTO.html]

Advanced IP Routing (Bandwidth control / Packet scheduling)
See chapter 11 in this howto for information on how to configure packet schedulers based on marked packets (see the RADIUS Filter-ID:qosmark attribute)
[http://www.tldp.org/HOWTO/Adv-Routing-HOWTO/index.html]

Variables

Variables can appear in html scripts and as parameters when calling server startup/shutdown, session start/stop and ping scripts. Variables begin with the '$' character, followed by the variable name. The values of variables are substituted for the '$' + variable name if available. If a value does not exist for a given variable then no substitution is done.

Variable	Description	HTML files	Start/Close scripts	Session scripts	Ping script
$error	Displays the contents of any error messages	Yes	No	No	No
login	Username form variable passed to the portal	N/A	N/A	N/A	N/A
password	Password form variable passed to the portal	N/A	N/A	N/A	N/A
referer	Referrer form variable passed to the portal	N/A	N/A	N/A	N/A
$replymsg	Auth response message	Yes	No	No	No

$user	Name of logged in user	Yes	No	No	No
$sessionid	Unique ID of current session	Yes	No	No	No
$timeleft	Amount of time remaining or 'Unlimited'.	Yes	No	No	No
$idletimeout	Displays the account's idle timeout setting	Yes	No	No	No
$timeon	Amount of time spent online so far	Yes	No	No	No
$referer	Original URL client was initially redirected from	Yes	No	No	No
$ip	IP Address of connected client	Yes	No	Yes	Yes
$mode	Session track mode 1=Gateway, 2=Routed	No	No	Yes	Yes
$serverurl	URL of the server	Yes	No	No	No
$redirecturl	Redirect URL	Yes	No	No	No
$interfaces	N/A	N/A	N/A	N/A	N/A
$routing	IP Routing mode 1=Static, 2=NAT	No	Yes	No	No
$serverport	HTTP Port the server is running on	No	Yes	No	No
$network	Network user gateway is configured for	No	Yes	No	No
$qosmark	Used to mark packets for bandwidth management.	No	No	Yes	No
$chain	Group portal related firewall rules using this label.	No	Yes	Yes	No
$authmethod	Password authentication method – 1=PAP, 2=CHAP	Yes	No	No	No
RADIUS:Filter-ID $*	See 'RADIUS attributes', allows for passing data to the session start/stop scripts via the RADIUS Filter-ID attribute.	Yes	No	Yes	No
$fwtype	Type of firewalling system used to control access and handle IP accounting. May be one of 'ipchains', 'iptables', 'ipfw', 'filterctl' or 'none'	No	Yes	Yes	No

Troubleshooting

The gateway can be configured to run in full debug mode when run with the following command line: ‘./portald –debug 255’. More debugging detail can also be enabled through the admin user interface and will appear in the message log file.

Checklist

General

- Make sure other applications are not listening on the default port (81) an alternate port can be used by starting the portal server with the parameters ‘-port x’ where x is the new port number.

- Required support packages are installed. (See system requirements) If running ‘portald –debug’ returns errors about missing shared object files a required package may need to be installed.

Linux platform

- IP Tables **or** IP Chains is installed and enabled. Typing ‘ipchains –L’ or ‘iptables –L’ should provide a list of fire walling rules currently configured. If there is an error running the command it must be fixed before the portal server will run correctly.

Windows platform

- For Windows, Air Marshal utilizes the IP Filter Driver interface to filter and redirect content. Only one filter driver may be active at any one time. Therefore, Air Marshal can not be installed onto a Windows computer that has another application using the IP Filter Driver.

Problems and Solutions

RADIUS

Problem. My RADIUS server is not getting auth or accounting requests from the gateway when logging into the authentication gateway.
Solution #1. Make sure the authentication and accounting port in the RADIUS server match the ones defined in the gateway configuration.
Solution #2. Make sure the RADIUS server is configured to allow RADIUS queries from the authentication gateway.

Problem. All authentication attempts fail, even after checking to see that the username and passwords are correct.
Solution. Passwords are encrypted using a shared secret. Secrets configured for the authentication gateway in the RADIUS server must exactly match the secret configured in the authentication gateway itself. If they don’t match… password decryption will fail causing a bad password error to be logged in the RADIUS server.

Problem. Authentication attempts fail when using CHAP authentication mode, but work correctly with the option disabled.

Solution. CHAP authentication requires the RADIUS server have access to the user's plain-text password. In some environments the user's password is encrypted in a way that make it impossible for the RADIUS server to decrypt. See your RADIUS server documentation for more information on CHAP authentication.

NAT/Routing (Linux)

Problem. Gateway process won't start, the debug output on my console or log file show there is a problem running the startup script.

Solution. Run the startup script '/usr/local/portal/scripts/startup.sh' from your shell prompt as root. This should help pinpoint the cause of the problem.

Problem. When NAT mode is enabled some applications outside of normal web browsing/ email stop working.
Solution. On the Linux platform kernel modules are available to allow protocols such as ftp, irc, streaming video and some multi-player games to work through NAT. See your operating system documentation for more information on NAT (IP Masquerade) and it's limitations.

Misc

Problem. Entries in the who's online display appear with a red background.
Solution. This can happen when one of the session scripts does not return successfully. Enable full debug to isolate which script or parameters are causing the problem and run that same command from your shell prompt. This should help pinpoint the cause of the problem.

Problem. On Windows, the user is never redirected to the authentication web server and they are allowed access without restriction.
Solution. Make sure the Air Marshal Filter Driver is installed and operating correctly. From a command prompt execute:

```
net start AirMarshalFilter
```

to start the filter driver. If the filter driver is either unknown or cannot start, see the section on installing the Windows Air Marshal Filter Driver.

Radius Attributes

Authentication

The following RADIUS attributes may be sent or received during an Access-Request/Accept.

RADIUS Attribute	Direction	Description
User-Name	Access-Request	This Attribute indicates the name of the user to be authenticated.

User-Password	Access-Request	PAP Password
CHAP-Password	Access-Request	CHAP Password
CHAP-Challenge	Access-Request	CHAP Challenge string
Session-Timeout	Access-Accept	This Attribute sets the maximum number of seconds of service to be provided to the user before termination of the session
Idle-Timeout	Access-Accept	Sets the maximum number of seconds a session can be idle before being terminated. Sending the idle timeout attribute disables active arp checking and the active ping script if one was defined for this session. Currently idle timeout is only supported in gateway mode.
Class	Access-Accept	Data received from this attribute during an Access-Accept is sent out in associated accounting – start/stop requests.
Filter-ID	Access-Accept	Used to pass parameters to the html and session start/stop scripts. Filter-ID is a text string consisting of "myvariable=myvalue". $myvariable contains the contents of myvalue.
Filter-ID:qosmark	Access-Accept	Filter-ID containing the string "qosmark=x" Where x is an integer value from 1 to 2^32. Used in tagging the IP address of the user to apply bandwidth management rules. See 'Customizing' for more information.
Filter-ID:htmlack	Access-Accept	Filter-ID containing the string "htmlack=filename" If specified filename is sent in place of ack.html after successful authentication.
Filter-ID:htmlstatus	Access-Accept	Filter-ID containing the string "htmlstatus=filename" If specified filename is sent in place of status.html to display session status.
Termination-Action	Access-Request	When 1 (RADIUS-Request) Air Marshal will send a new authorization request when Session-Timeout expires. If the authorization fails the session will be disconnected, otherwise the session will be re-authorized.

Accounting

The following RADIUS attributes may be sent in an Accounting-Request.

RADIUS Attribute	Description
Acct-Status-Type	Marks this Accounting-Request as the start/stop of a user session. 1=Start, 2=Stop.
Acct-Delay-Time	This attribute indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request.
Acct-Input-Octets	This attribute indicates how many octets have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
Acct-Output-Octets	This attribute indicates how many octets have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
Acct-Input-Gigawords	This attribute indicates how many times the Acct-Input-Octets counter has wrapped around 2^32 over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
Acct-Output-Gigawords	This attribute indicates how many times the Acct-Output-Octets counter has wrapped around 2^32 over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
Acct-Input-Packets	This attribute indicates how many packets have been received from the port over the course of this service being provided to the user, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop
Acct-Output-Packets	This attribute indicates how many packets have been sent to the port over the course of this service being provided to the user, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop
Acct-Terminate-Cause	This attribute indicates how the session was terminated, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop. 1=User Request, 3=Lost Service, 5=Session timeout, 6=Admin reset, 10=NAS Request, 11=NAS Reboot, 13=Port Preempted
Class	Class contains any data sent in the Class attribute during the Access-Accept for the users session.
Acct-Session-Id	This attribute is a unique Accounting ID to make it easy to match start and stop records.
Acct-Session-Time	This attribute indicates how many seconds the user has received service for, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

NAS-Port	This attribute indicates the virtual port number of the portal server the user has attached to.
Connect-Info	This attribute currently indicates the network interface the client was attached to. Additional information may be available via the Connect-Info field in the future.
NAS-Identifier	This Attribute contains a string identifying the NAS originating the Access-Request.
NAS-IP-Address	This Attribute indicates the identifying IP Address of the NAS originating the Access-Request.
Calling-Station-Id	(Caller ID) MAC Address of the client, if available.

Credits

SSL features based on the OpenSSL project (http://www.openssl.org)
MD5 compliments of RSA Data Security, Inc
MD5 JavaScript implementation by David West
Air Marshal Auth Gateway Programming & Documentation by IEA Software, Inc