Air Marshal

Authentication Gateway

Version 2.0.65

IEA Software, Inc.

SOFTWARE LICENSE AGREEMENT

By purchasing or installing all or part of the Emerald Management Suite, 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 Emerald Management Suite (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 Master Billing Records (MBRs) with 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 Agreement, 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., Emerald, RadiusNT, and the associated logo(s) are registered trademarks.

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 IEA Software's option, either

(a) return of 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.

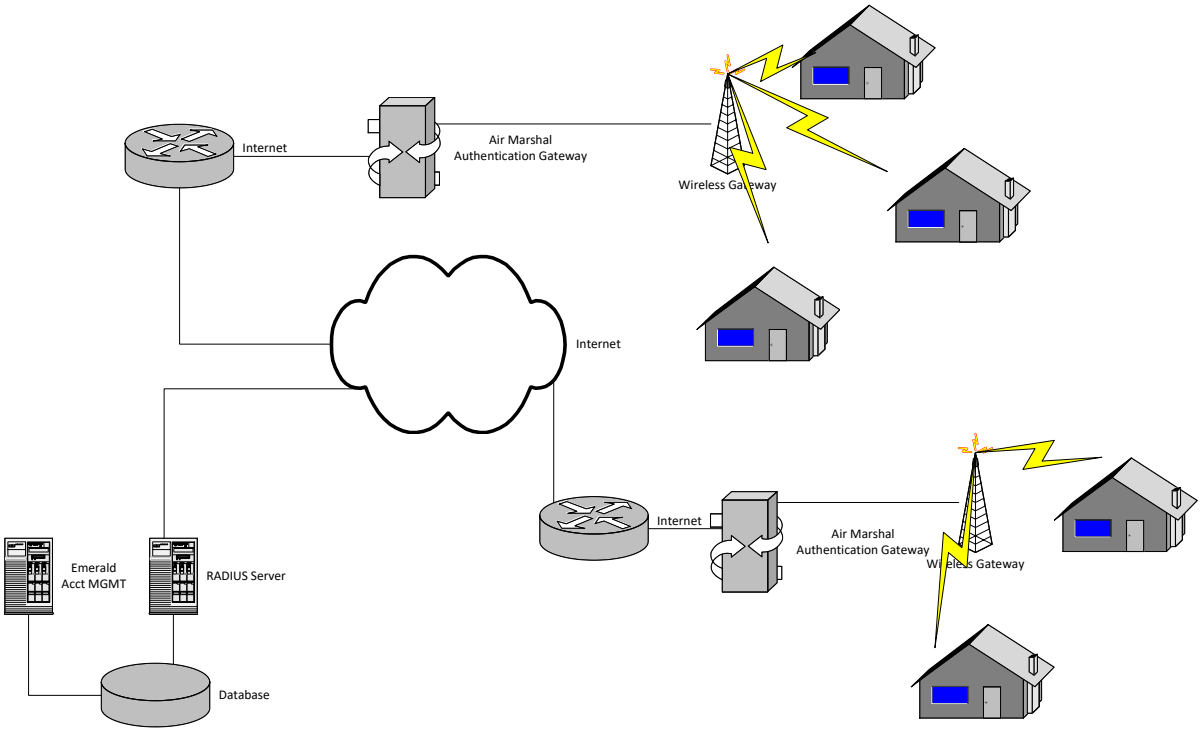
Should you have any questions concerning this license agreement, please contact IEA Software, Inc. PO BOX 1170 Veradale, WA 99037 U.S.A. (509) 444-BILL (2455).

TABLE OF CONTENTS

INTRODUCTION

Authentication gateways, sometimes called access controllers or captive portals provide an inexpensive simple way for the customer to obtain Internet access without having to install or configure software. Simply plug-in and the customers 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 and work the same in wired or wireless environments.



ABOUT IEA SOFTWARE

IEA Software, Inc is a world-leading provider of billing, customer care, and authentication solutions for ISPs, WISPs and VISPs. Please visit our web site (https://www.iea-software.com) or contact our sales staff at +1 509-444-BILL (2455) or sales@iea-software.com to learn more.

SECURITY CONSIDERATIONS

Authentication gateways are responsible for controlling access to the network. There is no additional security provided by Air Marshal to protect the integrity or confidentiality of Ethernet layer (Layer 2) data moving over the local network. However Air Marshal is able to protect confidential customer information such as account passwords entered through its client facing web interface by using industry standard TLS encryption technology.

Typically in an Internet access setting users will connect to TLS encrypted sites to access confidential information such as an online banking site or use encrypted VPNs to access resources on corporate networks. Since data moving across the Internet can be intercepted at any point along the way the only secure solution for data transmitted over the Internet are 'End-to-End' encryption technologies such as those employed using TLS and VPNs.

If Layer 2 encryption of traffic is required these solutions can be implemented alongside Air Marshal. For wireless networks we recommend using a RADIUS solution such as RadiusNT/X that provides 802.1x EAP-PEAP authentication and session encryption keys required to securely authenticate and establish encrypted WPA sessions. Additionally an access point supporting WPA + RADIUS is required.

Air Marshal provides a unique solution for preventing a user's password from being sent in the clear to mitigate the effects of TLS certificates not being used. The solution is CHAP based utilizing JavaScript to encrypt password data at the browser before being sent over the network to Air Marshal. As with most CHAP based solution it is vulnerable to offline dictionary attack against weak access passwords. We strongly recommend the purchase and use of TLS certificates to properly protect user credentials and other sensitive information. Small operations that may not want to purchase commercial TLS certificates have the option of creating self-signed certs and installing them manually in their browsers.

SYSTEM REQUIREMENTS

- Optional RADIUS server for client authentication and accounting.
- Any distribution of 64-bit Linux supporting kernel version 2.6 or higher.
- iptables and tc
- x64 based processor
- Computer must have 2 or more network interface cards installed.

LINUX INSTALLATION

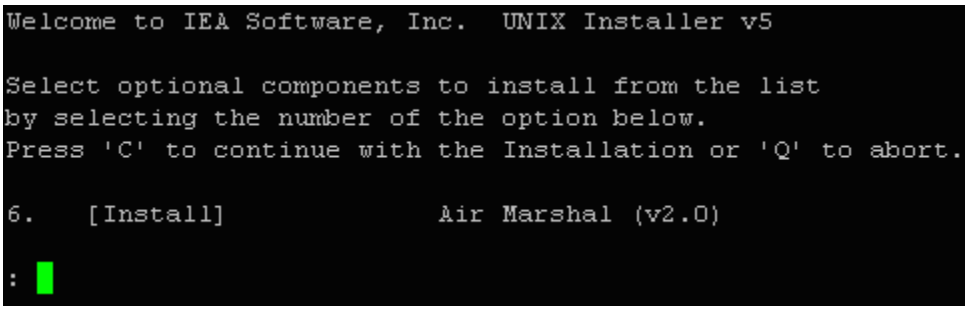
Download the Air Marshal archive (airmarshalv2_linux.tar.gz) into a temporary folder.

To un-archive the file type:

```
tar -zxf airmarshalv2_linux.tar.gz
```

Next, run the installer:

```
./install.pl
```



Press ‘C’ followed by return.

The Air Marshal 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:

systemctl disable portald

To re-enable automatic startup:

Systemctl enable portald

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.

Once server has been configured click ‘Save’ to complete server startup. 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:

systemctl start portald

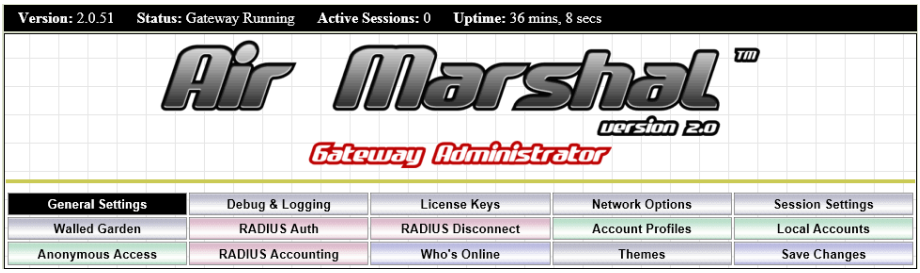
TRANSPORT LAYER SECURITY (TLS) CONFIGURATION

Air Marshal supports TLS encryption. To enable TLS and manage server certificates click ‘TLS certificate wizard’ from General Settings menu and follow on-screen instructions.

SERVER CONFIGURATION

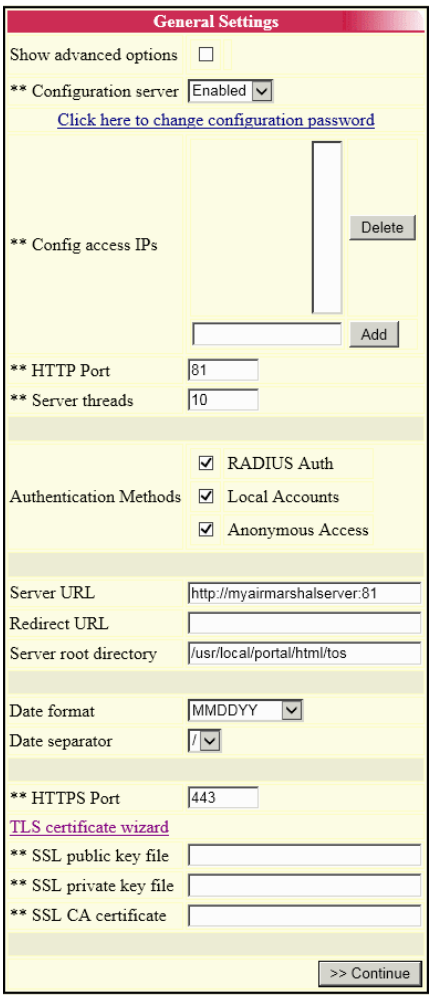
To configure and manage Air Marshal using a web browser access Air Marshal web interface located by default at **http://replacewithaddressofmyairmarshalserver:81/settings**

You will be presented with the gateway administrator menu.



Initially the available menu options will not show many of the items displayed in the picture above and the gateway status in the status bar at the top of the screen shows 'Not Started'. This indicates Air Marshal has not yet been fully configured and is not able to process login requests from clients. To configure Air Marshal at the very minimum you must review the General Settings and Network Options sections below to properly configure Air Marshal for your network. Once configured click 'Save Changes' to verify configuration and begin processing client requests. If validation fails you will be presented with an error message to correct any errors and try again. Once the Status bar displays 'Gateway Running' Air Marshal is active and able to process network login requests.

General Settings



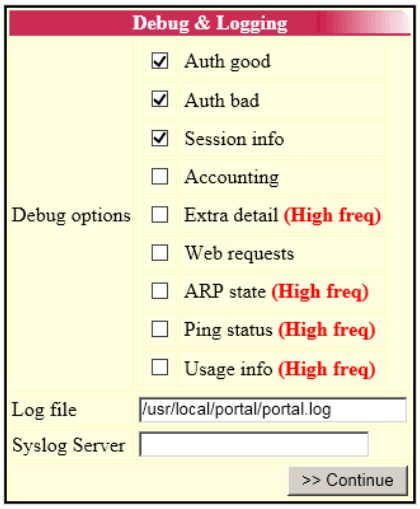
Option	Comments
Show advanced options	When checked all available advanced options are displayed in the Air Marshal administrator. When un-checked advanced options are hidden from view. Changing an advanced option is normally unnecessary and should not be done without direction from your support representative. This document assumes advanced options are disabled.
Configuration server	Controls whether or not the configuration server is accessible while the Air Marshal server is running. If this option is disabled the configuration server can be enabled when needed by starting the server with the flag '–config'
Config access IPs	Provides IP access restrictions to this configuration interface (/settings URL). If no IP Addresses are defined this interface may be accessed from any location by an operator with knowledge of the configuration password. If one or more access IP Addresses are configured this configuration interface is accessible only from one of the specified addresses. Access to the configuration UI from any other IP address results in an access-forbidden message. If necessary the Configuration access IP address list can be cleared manually

	from outside of the configuration UI by taking the following steps: Open /usr/local/portal/portal.ini using a text editor. Remove line starting with **ConfigAccessIP=** Stop and restart the server
HTTP Port	HTTP Port this server will listen for requests. While the default port is 81 using the standard HTTP port of 80 allows local DNS aliased shortcuts such as typing 'status' or 'logout' in the browsers URL field to work.
Server threads	Number of concurrent web accesses the server can handle at a time. The default value is 50 and maximum allowable is 1024. Each thread requires an additional 600k of virtual memory.
Authentication Methods	Provides selection of available authentication methods for client authentication. See Radius Auth, Local Accounts and Anonymous Access for more information on each authentication method.
Server URL	URL of this server from the perspective of the clients accessing air marshal for authentication. For example http://10.0.8.254:81/ The HTTP Port must be included in the Server URL if it is set to something other than the default http port 80. If TLS is enabled the Server URL field should reflect the https address of this server.
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. Note: If the WISPr-Redirection-URL RADIUS attribute is available it takes precedence over this option.
Server root directory	Root directory under which the html files for the administrative and authentication web interfaces can be found. Two separate sets of logon interfaces are included and can be selected by changing the Server root directory between the two. **/usr/local/portal/html/default** Provides a "classic" Air Marshal login page with limited support for pre-authentication. **/usr/local/portal/html/tos** Provides an alternate Air marshal login page explicitly allowing the user to choose between guest and authenticated access. It also presents terms of service the user must accept before they are able to authenticate. Dummy links to new account signup servers and customer self-management URLs based on Emerald v6 is also provided.
Access-Control-Allow-Origin	Overrides restrictive default Cross Origin Resource Sharing (CORS) policy to allow third party websites to programmatically access Emerald via client browser system wide for all ews requests. If specified value entered here (Normally * or https://mytrustedsite.example) is transmitted as header value within http response. If not specified Access-Control-Allow-Origin and Access-Control-Allow-Credentials headers are not transmitted in http response. Option is visible only while show advanced options in General Settings is enabled.
Date format	Allows configuration of local date format for display and manipulation of expiration dates in the Local Accounts menu.

Date separator	Allows configuration of local date part separator for display and manipulation of expiration dates in the Local Accounts menu.
HTTPS Port	If using TLS this is the https port the server will listen for TLS requests.
TLS Versions	Controls TLS version availability during TLS version negotiation between Air Marshal server and client browser.
TLS public key file	File containing this sites base64 encoded public key. Please see the certificate wizard for details.
TLS private key file	File containing this sites base64 encoded private key. Please see the certificate wizard for details.
TLS CA certificate	File containing the CA's certificate chain or intermediate certificate bundle in base64 format. Follow your CA's documentation to obtain this file.

Debug & Logging

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



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 user's 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 Air Marshal. 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.
Accounting Log	N/A	File to log session accounting start and stop messages for sessions

File		authenticated through Air Marshal. Note: The accounting log file is only available as an option and written to disk if RADIUS Accounting is not configured.
Log file	N/A	Filename to write the log output.
Syslog Server	N/A	IP Address or DNS hostname of the syslog server to logging messages are to be written. All messages are sent to the local4 logging facility. If the DNS name has multiple addresses copies of the message are sent to each IP address associated with the DNS name.

Licensing

Please contact our sales department +1 509 444 2455 option 1 or sales@iea-software.com for an Air Marshal license key.

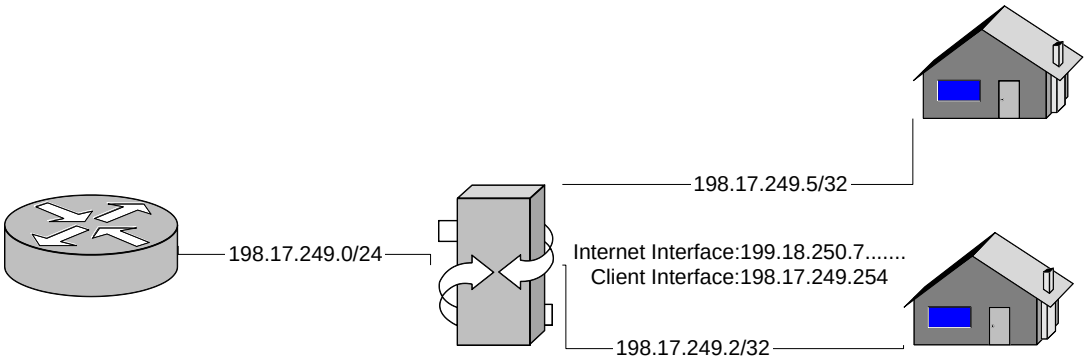
```
You may use up to one copy of Air Marshal throughout your organization
limited to 5 concurrent sessions at no cost without obtaining a license key.
```

Network options

Network interfaces and subnets controlled by the authentication gateway are configured through the network options menu. There are three available network routing technologies available depending on your needs. Information on each network routing option is available from the IP Routing, Network Address Translation and IP Bridging sections below.

IP Routing (Layer 3)

In IP routing mode IP address blocks are routed to the Air Marshal server for use by the end users (client) accessing the network. This method is typically used when there is a need to assign the client Internet routable IP address.



Routing mode requires that the relevant subnets are routed to the Air Marshal server and the managed client facing network interface(s) on the Air Marshal server have been properly configured.

Additionally you will need a method of dynamically assigning IP Addresses to clients accessing the network through Air Marshal. This is typically handled either by the devices that connect the client to the network (Such as wireless access points) or by running a DHCP server configured to assign addresses from the appropriate network blocks.

We recommend before installing Air Marshal on the server for the first time the server is tested to ensure clients connecting to the network have full access to the Internet or internal networks without the Air Marshal software installed. Following this approach allows you to troubleshoot any internal routing problems separate from the network filtering services provided by Air Marshal.

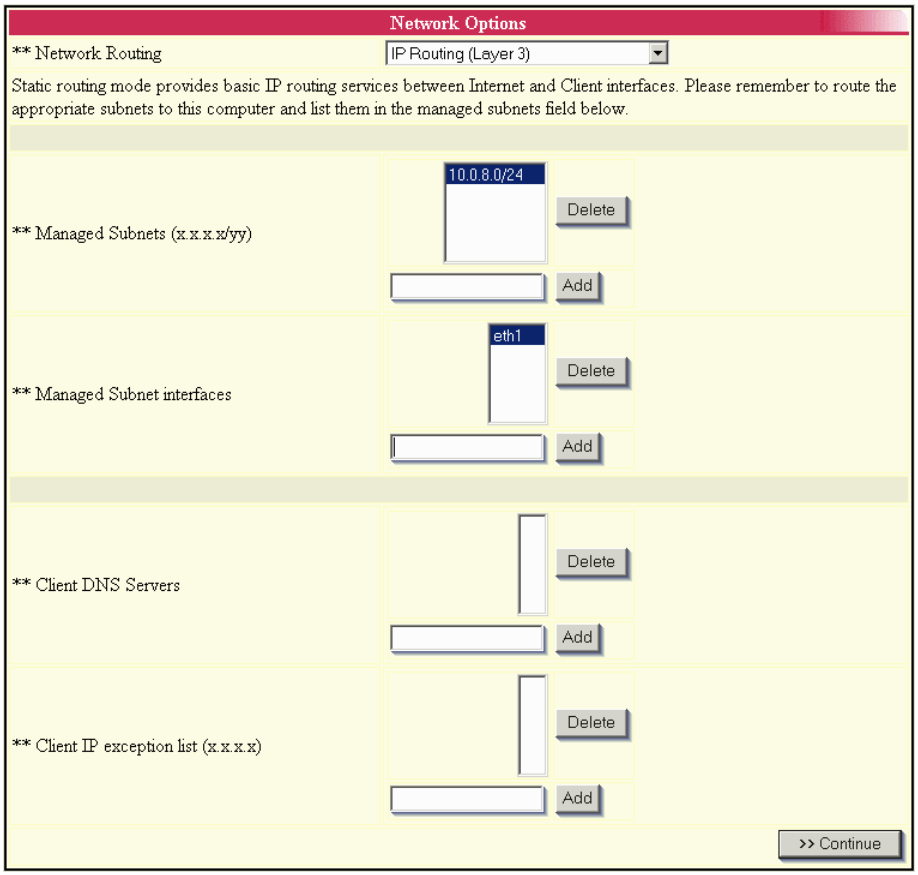
If Air Marshal has already been installed and configured you can stop the Air Marshal process and then clear all fire walling and filtering rules from the system by running the following commands:

iptables –t nat –F

iptables –F

iptables –t mangle –F

If clients cannot access the network when IP Routing mode is desired you know there is a routing or configuration problem not related to the Air Marshal server.



Option	Description
Scalable filtering	When enabled average packet processing costs of per-session filtering rules remains fixed as number of active concurrent sessions increase. An increasing performance benefit is realized as number of concurrent sessions increase beyond 100. Enabling scalable filtering significantly increases initial Air Marshal startup time and offers no performance advantages below 50 concurrent sessions.
Per session NAT port allocation	This setting is used to manage traceability of individual clients behind a single IP address in NAT routing mode. When the recommended default of "Dynamic" is selected ports are allocated randomly across all sessions making it impossible to later trace source port to an individual session. When set to 5 or more selected number of ports is uniquely assigned to each concurrently active session such that assigned port range is not shared with any other active session. The higher the number of ports allocated to an individual session the lower maximum number of concurrent sessions the system is able to manage. With each selection the maximum number of concurrent sessions is indicated. Low number of source port restricts total number of simultaneous TCP and UDP sessions able to be established to any single host and single destination port.

	When enabled the NAS-Port-Id attribute is transmitted in RADIUS authentication and accounting messages instead of NAS-Port. This value is formatted as "1024-1034" reflecting the starting and ending port of the allocated port range.
Internet interface	Interface providing Air Marshal access to the Internet or internal network. Note: Internet interface is not the client facing interface (See Managed Subnet interface below)
Internet Download Bandwidth	Applies a global shared download bandwidth limit to all user sessions per managed subnet interface constraining network bandwidth to the rate configured in kilobits per second. This should represent the smaller of the networks non-burstable download capacity or the maximum bandwidth administratively allocated to each managed subnet interface. If the limit is used to provide prioritization for an oversubscribed channel the bandwidth should be set slightly lower than the actual capacity of the channel. If both download and upload bandwidth parameters are left blank no per managed subnet interface bandwidth limit is enforced. If only one of the two is set the set value applies to both download and upload.
Internet Upload Bandwidth	Applies a global shared upload bandwidth limit to all user sessions constraining total systems network bandwidth to the rate configured in kilobits per second. This should represent the smaller of the networks non-burstable upload capacity or the maximum bandwidth administratively allocated to the system. If the limit is used to provide prioritization for an oversubscribed channel the bandwidth should be set slightly lower than the actual capacity of the channel. If both download and upload bandwidth parameters are left blank no global bandwidth limit is enforced. If only one of the two is set the set value applies to both download and upload.
Managed Subnets	List of Ipv4 subnets in CIDR notation (x.x.x.x/y) that will be managed by Air Marshal where authentication and redirect services will be provided.
Managed Subnet interfaces	List of physical interfaces connecting the client to the managed subnets listed above. Note: If you have configured virtual interfaces such as eth1:x only the actual physical interface name should be specified.
Client DNS Servers	If Client DNS Servers are specified DNS server access to clients that have not been authenticated through Air Marshal is restricted to this list of servers. If no Client DNS Servers are specified the client can contact any DNS server available on the network before they have successfully authenticated. We recommend not specifying a Client DNS server for maximum client compatibility.
Client IP exception list	List of IP addresses falling within the managed subnet range defined above that should be excluded from authentication and redirect services provided by Air Marshal.

Network Address Translation (NAT)

Network address translation is useful when you need to provide many clients Internet or internal network access however very few Internet routable IP addresses are available. When used clients are assigned addresses from one of the designated non-routable IP address blocks. The Air Marshal server then shares its network connectivity with all connected clients using network address translation (NAT).

To use this routing mode configure the client facing network interface(s) with a non-routable network.

All of the following network ranges are reserved for internal networks and available for use:

10.0.0.0 (Class A)

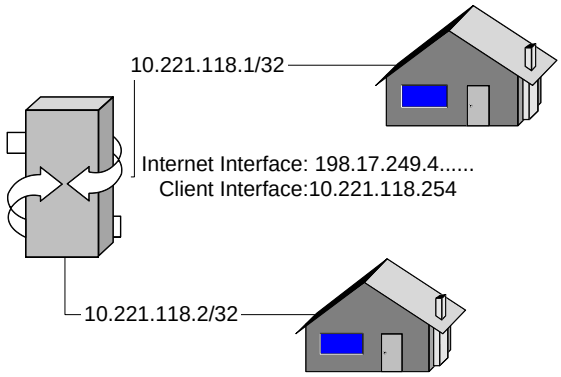
172.16.0.0 – 172.31.0.0 (Class B)

192.168.0.0 – 192.168.255.0 (Class C)

If you are providing Internet access for the public choose subnets that are not likely to be used in other private networks such as those used internally throughout many corporate IP networks. Following this advice prevents possible IP routing conflicts between the services you are providing to the client and any corporate network the client may connect to using VPN technology.

For example do not use the top or bottoms of any of the private subnet range or identifiable patterns of a particular range such as 10.10.10.0/24. In particular 10.0.0.0/24 should not be used. Examples of better choices are 10.221.118.0/24 or 10.158.0.0/16

After you have assigned IP address to the client facing network interface(s) you will need to configure a DHCP server or access hardware (Such as a wireless access point) to assign addresses from the configured client network range. The default route assigned to the clients must match the IP address assigned to the client facing network interface on the Air Marshal server. For example:



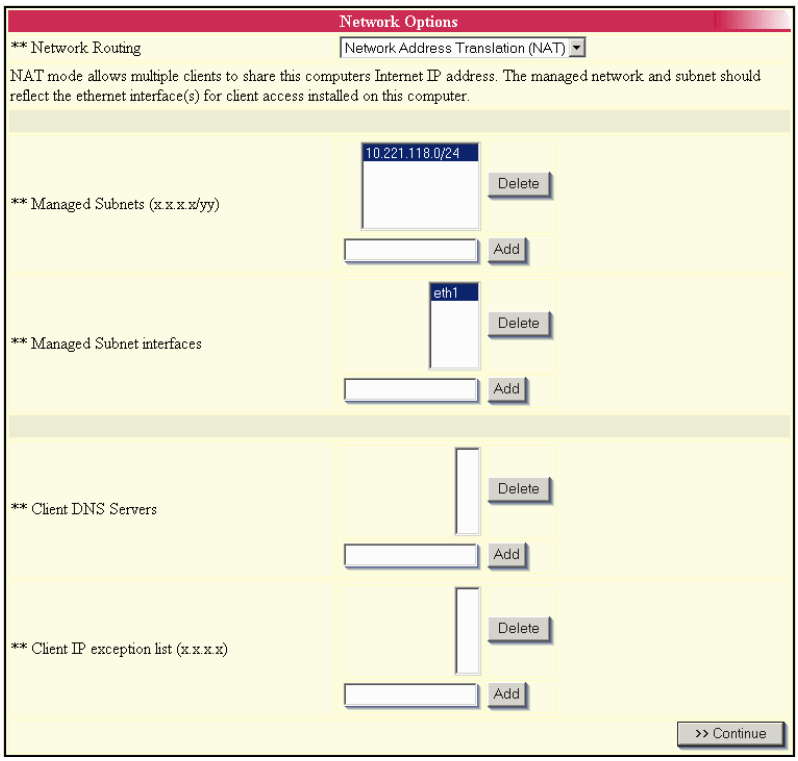
eth1 is the client facing Ethernet interface. It is using the network **10.221.118.0/24.**

eth1 is assigned the address **10.221.118.254** with a netmask of **255.255.255.0**

The DHCP server would be configured to assign addresses to clients within the range 10.221.118.1 thru 10.221.118.253.

DHCP would also assign clients the default route of the client interface on the Air Marshal server 10.221.118.254.

This is the only configuration necessary for NAT. Air Marshal will enable NAT and handlers to allow many popular applications to continue to operate in the NAT environment.

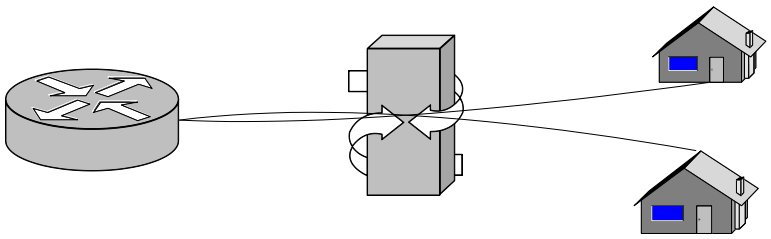


Option	Description
Internet interface	Interface providing Air Marshal access to the Internet or internal network. Note: Internet interface is not client facing interface (See Managed Subnet interface below)
Internet Download Bandwidth	Applies a global shared download bandwidth limit to all user sessions per managed subnet interface constraining network bandwidth to the rate configured in kilobits per second. This should represent the smaller of the networks non-burstable download capacity or the maximum bandwidth administratively allocated to each managed subnet interface. If the limit is used to provide prioritization for an oversubscribed channel the bandwidth should be set slightly lower than the actual capacity of the channel. If both download and upload bandwidth parameters are left blank no per managed subnet interface bandwidth limit is enforced. If only one of the two is set the set value applies to both download and upload.
Internet Upload Bandwidth	Applies a global shared upload bandwidth limit to all user sessions constraining total systems network bandwidth to the rate configured in kilobits per second. This should represent the smaller of the networks non-burstable upload capacity or the maximum bandwidth administratively allocated to the system. If the limit is used to provide prioritization for an oversubscribed channel the bandwidth should be set slightly lower than the actual capacity of the channel. If both download and upload bandwidth parameters are left blank no global bandwidth limit is enforced. If only one of the two is set the set value applies to both download and upload.

Managed Subnet interfaces	List of physical interfaces connecting the client to the managed subnets listed above. Note: If you have configured virtual interfaces such as eth1:x only the actual physical interface name should be specified.
Client DNS Servers	If Client DNS Servers are specified DNS server access to clients that have not been authenticated through Air Marshal is restricted to this list of servers. If no Client DNS Servers are specified the client can contact any DNS server available on the network before they have successfully authenticated. We recommend not specifying a Client DNS server for maximum client compatibility.
Client IP exception list	List of IP addresses falling within the managed subnet range defined above that should be excluded from authentication and redirect services provided by Air Marshal.

Bridging (Layer 2)

Bridging involves merging multiple networks together at the Ethernet layer. With bridge mode Air Marshals internal and client facing interfaces are combined creating a single Ethernet segment. Air Marshal then transparently applies redirect and authentication services to data moving through the bridge.

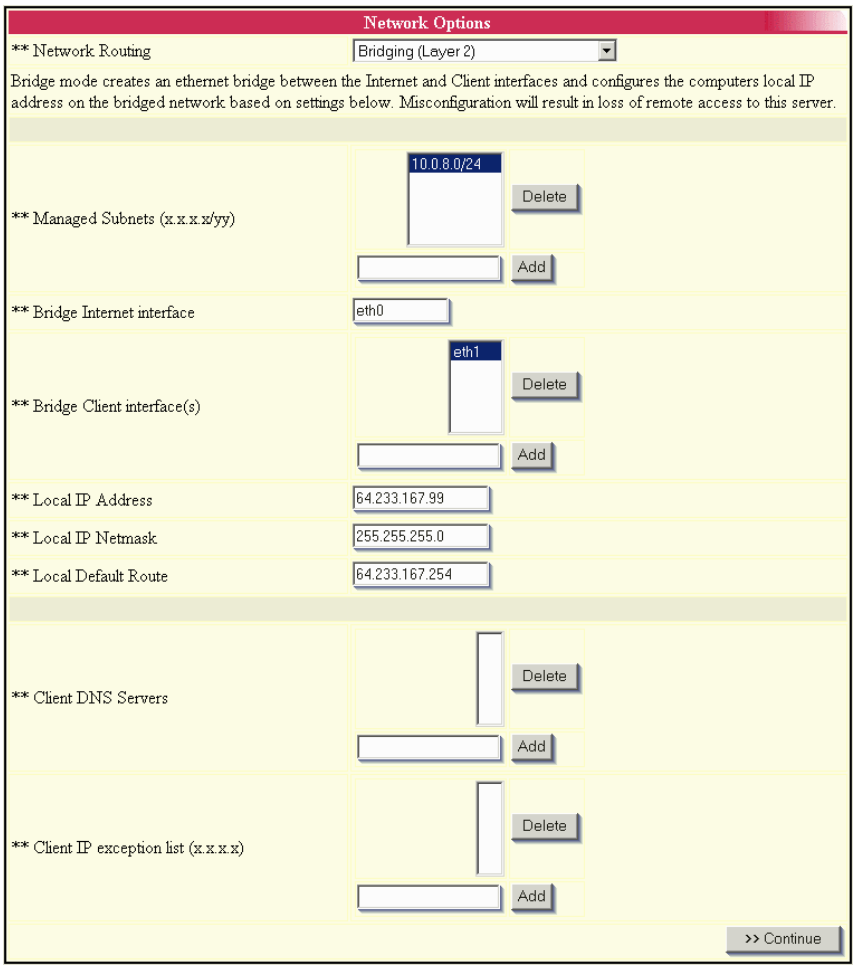


Bridging has the advantage that it allows Air Marshal to be 'plugged in' to an existing network without having to make any external configuration changes to the network.

Bridge mode has the disadvantage of sharing the same network broadcast scope between all participants. Additionally data rate limits are not enforced when bridge mode is enabled.

When the bridge routing mode is enabled Air Marshal removes the current configuration of all participating Ethernet interfaces and bridges them together. During this step the computer is assigned the IP address, netmask and default gateway configured from the network options menu as shown below.

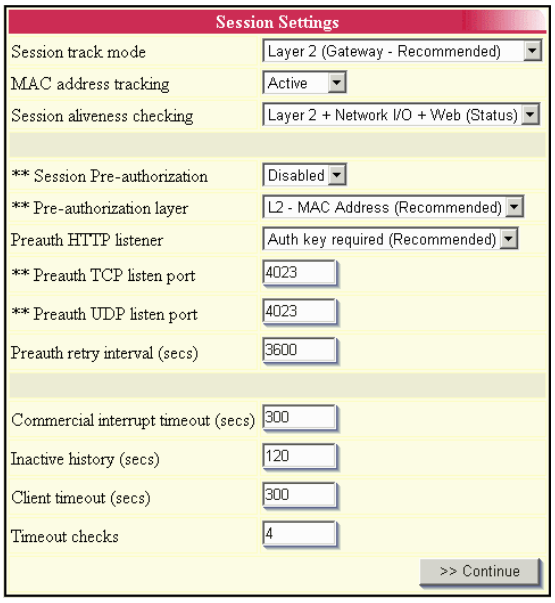
The Linux 'brctl' utility is required to enable bridging. On most modern linux distributions it can be installed by typing 'yum install bridge-utils' or 'apt-get install bridge-utils' from a shell prompt.



Option	Description
Managed Subnets	List of Ipv4 subnets in CIDR notation (x.x.x.x/y) that will be managed by Air Marshal where authentication and redirect services will be provided.
Bridge Internet interface	The Ethernet interface connected to the internal or Internet network.
Bridge Client interface(s)	List of physical interfaces connecting the client to the Air Marshal server.
Local IP Address	After the Ethernet bridge is established this reflects the Air Marshal servers local IP address on the bridged network.
Local IP Network	After the Ethernet bridge is established this reflects the Air Marshal servers local IP netmask on the bridged network.
Local Default Route	After the Ethernet bridge is established this reflects the Air Marshal servers Local default route on the bridged network.
Client DNS Servers	If Client DNS Servers are specified DNS server access to clients that have not been authenticated through Air Marshal is restricted to this list of servers. If no Client DNS Servers are specified the client can contact any DNS server available on the network before they have successfully authenticated. We recommend not specifying a Client DNS server for maximum client compatibility.
Client IP exception list	List of IP addresses falling within the managed subnet range defined above that should be excluded from authentication and redirect services provided by Air Marshal.

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 client's connection during the course of their session are configured through this menu.

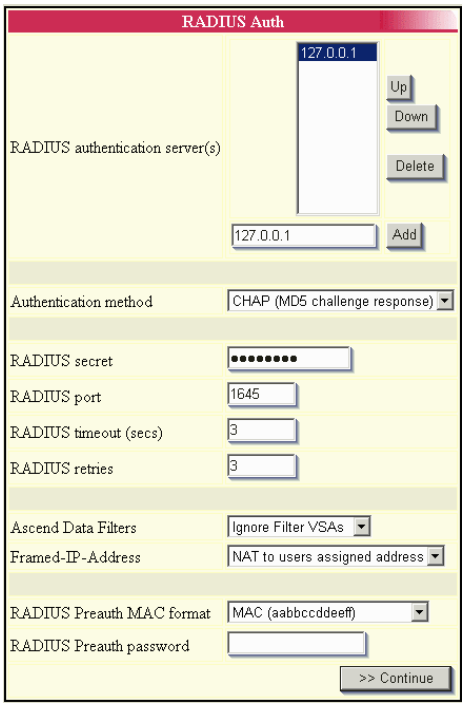


Option	Description
Session track mode	Layer 2 is recommended and assumes all clients are connecting through the same physical network. This mode allows the collection of client MAC information. Layer 3 assumes all clients are accessing the network through a secondary IP router. If there are a mix of directly connected and routed users on the network – select the 'Layer 2' mode. If Layer 3 mode is enabled the client UI popup status window is required to keep client sessions from timing out.
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'.
Session aliveness checking	Listing of methods used in detecting continued presence of a session. **Method** / **Description** Layer 2 – Session status refreshed by client response to network layer ARP requests. If Session track mode is Layer 3 this method will NOT be used for session tracking. Network I/O – Session status refreshed by new data sent from the client computer. Web (Status) – Session status refreshed by access to the Air Marshal web status popup.
Session Pre-authorization	When 'Enabled' Air Marshal is able to authenticate clients automatically

	without the user having to enter their login and password based only on the MAC or IP address of client's computer. Session Pre-Authorization must be enabled in order for Anonymous Access to work. Session Pre-authorization is also supported for local accounts and RADIUS based authentication. For local accounts the MAC address must be entered into the login field. For RADIUS based authentication the MAC or IP address is sent as both the username and password or a single Pre-authorization password can be set from the RADIUS Auth menu. A session track mode setting of Layer 2 is required for MAC based session pre-authorization.
Pre-authorization layer	If session pre-authorization is enabled the setting selects layer 2 MAC address or layer 3 IP Address to be used as keys for session pre-authorization. This setting applies only for RADIUS based authentication and has no effect on Anonymous authentication or authentication using local accounts. It is recommended MAC address be used whenever possible for session pre-authorization.
Preauth HTTP listener	When set to 'Auth key required' preauthorization from the web client login interface requires authorization key to be provided via the client UI to authenticate using the pre-authorization method. When set 'Any HTTP request' all http requests received by Air Marshal may be used to trigger pre-authorization. This setting may be used to support pre-authentication for network enabled devices which do not have an interactive web browser and may only use the HTTP protocol to access the network.
Preauth TCP listen port	Sets the TCP protocol listener port Air Marshal is to listen on to Pre-authorize sessions making a non-web based outgoing TCP connection. If you want to force pre-authorization through the web interface set the TCP and UDP listen ports to 0 to disable this feature.
Preauth UDP listen port	Sets the UDP protocol listener port Air Marshal is to listen on to Pre-authorize sessions making a non-web based outgoing UDP request. If you want to force pre-authorization through the web interface set the TCP and UDP listen ports to 0 to disable this feature.
Preauth retry interval	Number of seconds after an initial failed preauthorization request to try again. Generally this should be set high enough that it will never occur. The 'inactive history' option below effectively controls the lifetime of stored sessions that are not in an active state. This setting should only be set if you need to retry preauthorization more aggressively than the inactive history setting below.
Commercial interrupt timeout	Whenever a commercial interruption message is displayed to the client this is the system wide default amount of time the client has to acknowledge the commercial message before their session is disconnected. Commercial interrupt can be set on a per user basis for sessions authenticating via RADIUS via the IEA VSA attribute AM-Interrupt-Timeout
Inactive history	The length of time inactive sessions should be kept in the "Who's Online" list after attempting to authenticate or becoming inactive.
Usage refresh	Interval at which byte count statistics for all open sessions are updated. Option is visible only while show advanced options in General Settings is enabled.
ARP refresh	Interval when a sessions ARP info is rechecked. Option is visible only while show advanced options in General Settings is enabled.
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.

RADIUS Auth

RADIUS authentication provides for centralized management of subscribers across all network access devices. Typically RADIUS is used for managing large numbers of accounts, participating in roaming networks or integrating with subscriber management and billing platforms such as Emerald.

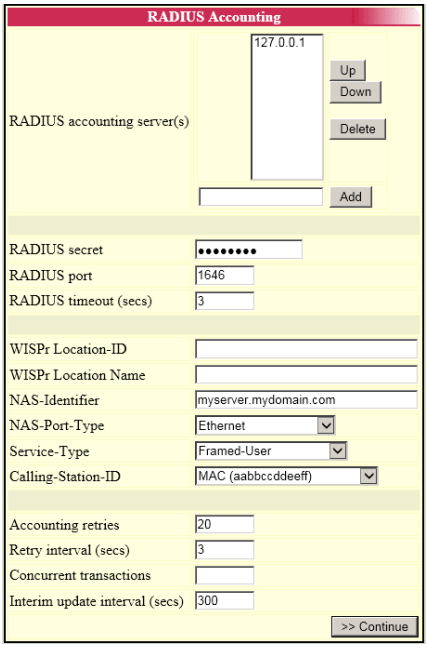


Option	Description
RADIUS authentication server	IP address/hostname of RADIUS authentication server. If Multiple servers are entered they are contacted in the order they appear if there was no response from the previous server. Note: All defined authentication servers share the same RADIUS port and secret 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 TLS be used to protect the client's password.
RADIUS secret	The shared secret is a type of password set the same between the RADIUS server and Air Marshal. It is recommended shared secrets be at least 16 characters in length containing a random mixture of mixed case letters, numbers and symbols.
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 whether an authentication server is available.
Ascend Data Filters	When set 'Accept' Ascend data filters sent in response to a clients RADIUS

	authentication request will be enforced. When 'Ignore' any Ascend data filters in the access accept are ignored.
Framed-IP-Address	When set 'NAT to users assigned address' the Framed-IP-Address RADIUS attribute is used to setup a one-to-one NAT association of the specified Framed-IP-Address to the users internal address. This feature is typically used to associate an external Internet routable IP-Address with the users internal DHCP assigned address allowing the users computer to be reached from the public Internet and all outgoing traffic to appear from the external public address assigned to this user. Note: Care should be taken to ensure the same Framed-IP-Address is never assigned to two different users at the same time. When set 'Ignore Framed-IP-Address' and a Framed-IP-Address is sent in the RADIUS access accept the attribute is ignored and no NAT association is performed.
RADIUS Preauth MAC format	When session Pre-authorization is enabled and preauthorization layer in session settings is set "L2 MAC" this option sets the format of the User-Name attribute sent with RADIUS Preauth requests.
RADIUS Preauth password	When session Pre-authorization is enabled this option sets the password sent with RADIUS Preauth requests. If this field is blank the password matches the MAC address of the client sent in the username field.

RADIUS Accounting

As clients logon and off RADIUS accounting records are used to store important information related to the services provided to each client such as the time spent online, amount of data traffic, IP, MAC and diagnostic information such as the reason each session was closed. This data is typically useful for wide array of tasks such as usage billing, enforcement of data and time limits, managing concurrent access, capacity planning, auditing and troubleshooting.



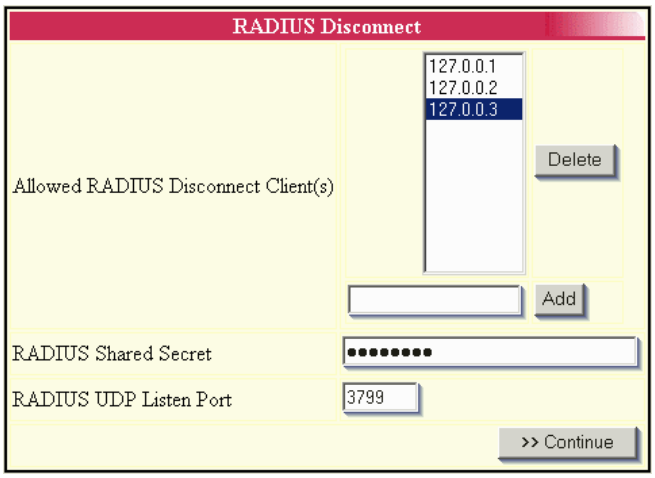
Option	Description
RADIUS accounting server	IP address/hostname of RADIUS accounting server. If Multiple servers are entered they are contacted in the order they appear if there was no response from the previous server. All defined accounting servers share the same RADIUS port and secret settings.
RADIUS secret	The shared secret is a type of password set the same between the RADIUS server and Air Marshal. It is recommended shared secrets be at least 16 characters in length containing a mixture of letters, numbers and symbols.
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.
WISPr Location-ID	Location-ID is used in roaming environments to identify the physical hotspot location the end user is connecting to.
WISPr Location Name	Location Name is used in roaming environments to identify the physical hotspot location the end user is connecting to.
NAS-Identifier	IP Address or hostname of this server, if a hostname is entered it is recommended to be resolvable via DNS.
NAS-Port-Type	NAS port type reported for informational purposes during RADIUS Access-Request and Accounting-Request to the RADIUS server. The default and recommended value is “Virtual”.
Service-Type	Service type reported for information purposes during RADIUS Access-Request and Accounting-Request to the RADIUS server. The defaulted and recommended value is “Framed-User”
Calling-Station-ID	Selects format and content of Calling-Station-ID attribute sent during RADIUS Access-Request and Accounting-Request to the RADIUS Server. If MAC is selected and MAC data is unavailable no Calling-Station-ID attribute is sent.
Accounting retries	Total number of unique attempts to deliver an accounting message before discarding it. The higher the retry count the better protected from loss of accounting due to loss of access to primary and secondary RADIUS accounting server(s). Note: Accounting retry counts are calculated as failures of the entire retry policy configured above including attempts to any backup accounting servers the ‘RADIUS timeout’ and ‘RADIUS retries’ setting. Therefore a single accounting retry typically involve several actual accounting requests, possibly across multiple servers.
Retry interval	Base retry interval between previous failed accounting attempts. Retry interval automatically increases from this base value after a number of failed attempts. This allows for longer periods where an accounting server is unavailable.
Concurrent transactions	Maximum simultaneous number of "in-flight" RADIUS accounting requests allowed pending at once. Valid values range from 1 to 255. Lower values result in decreased load on RADIUS servers at expense of reduced throughput. Higher values may significantly improve throughput over high latency networks at expense of periods of increased load on RADIUS server. By default when left empty concurrent transaction limit is managed

	automatically.
Interim update interval	Interim updates are accounting messages that provide updated information on the state of active sessions such as the amount of data used thus far. Interim updates are optional and should only be enabled if there is a specific need such as enforcement of data usage limits. If this field is left blank Interim updates are disabled by default otherwise the field sets the default number of seconds between interim accounting updates for each session. A setting of less than 5 minutes (300 seconds) is not recommended. If the RADIUS attribute Acct-Interim-Interval is sent in response to an authentication request its value overrides the system default.

RADIUS Disconnect

Occasionally there may be a need to disconnect active sessions due to unexpected changes in account status based on information not available at the time a client session was started. As an example a customer may prepay for a months of service with a check. The customer is granted access for a month's time and logs on. However later you receive notification there were insufficient funds to honor the check. Since access was already granted and the customer is online 'Disconnect' provides a means to force the customer to logoff and provide alternate payment.

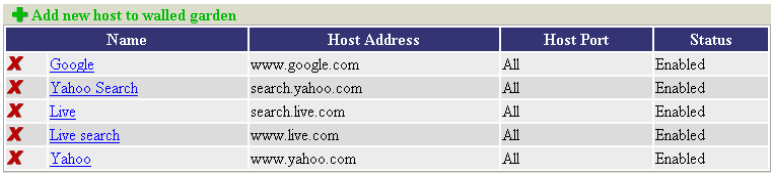
Disconnect is typically used for enforcement of access restrictions in complex situations where a single account may be allowed to be shared by multiple people simultaneously and there are requirements for enforcement of account balance and or data based rate plans that cannot be conveyed exclusively through limits set via RADIUS authorization attributes. Disconnect messages are typically initiated through an RFC3576 compliant management server such as the Emerald session manager however you may also initiate Disconnect requests manually using Air Marshals who's online view or tools such as the 'RADIUS test client' available from the IEA Software web site: https://www.iea-software.com/radlogin



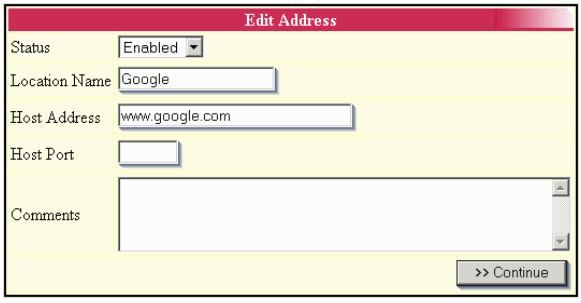
Option	Description
Disconnect Clients	List of hosts allowed to send disconnect requests to Air Marshal. Requests from any clients not on this list are ignored.
Shared Secret	Shared secret used to validate and protect disconnect requests. The shared secret is a type of password set the same between authorized disconnects clients and Air Marshal. It is recommended shared secrets be at least 16 characters in length containing a mixture of letters, numbers and symbols.

UDP Listen Port	This sets the UDP port Air Marshal is to listen for disconnect requests. The official port reserved for RADIUS disconnect is 3799 however UDP port 1700 is still widely used by Cisco and others.

Walled Gardens



Typically prior to logging on clients have no access to network resources. The walled garden enables exceptions so that clients not having logged on are still able to access certain resources. Examples of exemptions included in typical walled gardens are new account signup and account management systems such as Emerald, access to your organizations web site, local business and other resources related specifically to your venue or location. Those operating a public hotspot in an Airport may want to provide free access to flight status and airline reservation web sites. Hotel operators may want to provide access to local restaurants and transportation services.



To add or manage existing hosts assigned to the walled garden choose the Walled Garden menu option.

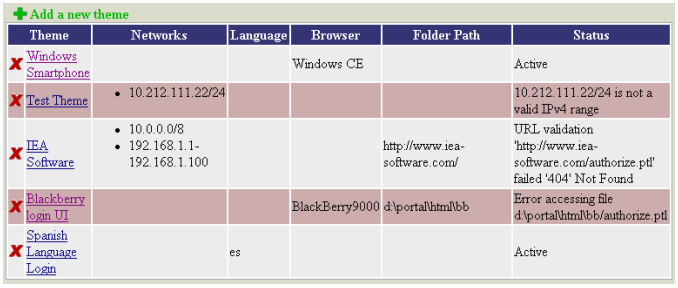
The walled garden menu will not appear if the Air Marshal server has not started. If the menu is not available choose 'Save Changes' and correct any configuration errors shown.

To add new sites select the 'Add new host' link. To make changes to an existing site click the site name from the listing or click the red 'x' to remove the site. If you are making several changes within a short period of time it may take up to 45 seconds for site changes to become effective.

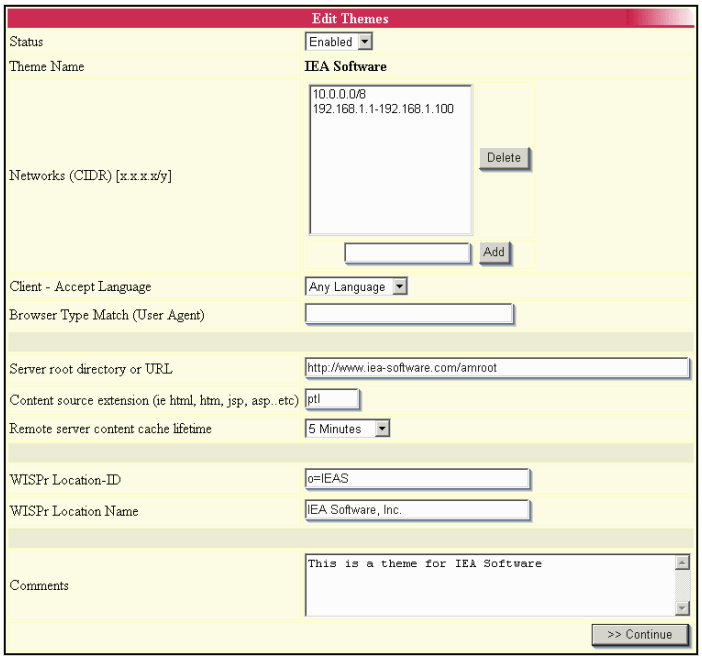
Option	Description
Status	When Enabled the site exception for the host is in effect, when Disabled the exception is not honored.
Location Name	A short plain text description of the site
Host Address	The IP address or hostname of the site being allowed. Note: This field must reflect a DNS resolvable hostname only. URLs or wildcards are not permitted as host addresses.
Host Port	The IP port number to restrict site access. For example to restrict access to only HTTP requests to a host you would enter 80 or 443 for HTTP and HTTPS respectively. If you want to allow full access to the site on all available ports leave the host port field blank.
Comments	Additional comments related to this site

Themes

Themes enable the systems client facing login screens to be tailored to uniquely match needs of users based on venue or client network, browser or device type and native language. Typical usage scenario include serving multiple venues with customized access portals for each or customizing user experience to concurrently target a variety of access technologies including mobile phones, consoles and notebook computers.



From a technical viewpoint themes conditionally set the equivalent of 'Server Root Directory' as normally configured in the General Settings menu to define the location of the user facing login portal. This folder may be located on the local server or a remote web server. See the Customizing section below for more information on required files and interface customization.



Option	Description
Status	While "Enabled" the theme is available to be selected for those clients matching conditions of the theme. When "Disabled" the theme is removed from availability.
Networks	List of end-user IP subnets in CIDR notation the theme is eligible to match. If no networks are configured the theme is not restricted to users based on their assigned IP Address. In addition to CIDR notation Ipv4 addresses can be specified as address ranges in the form 'x.x.x.x-y.y.y.y' with minus sign between the starting and ending ranges. For example 192.168.1.10-192.168.1.20 allows all addresses falling within the range to be used. If multiple themes share overlapping networks and have the same specificity with regards to Accept Language and Browser Type (see below) the theme with the most specific network definition will be selected. For example:

<table>
<tr><td></td><td>Theme A: 10.0.0.0/8
Theme B: 10.0.0.0/24

User with IP Address 10.0.0.115 matches both themes A and B. However because “Theme B” specified a more specific network it will be preferred over “Theme A”.</td></tr>
<tr><td>Accept Language</td><td>Many web browsers allow users to define a set of languages they understand in order of preference. These settings serve to signal to web sites the users preferred language when presenting content. If accept language is set a theme will only match if the user has the listed language configured in their browsers accept language list.

If you choose to make available language specific themes it’s recommended a theme be configured explicitly for each specific language supported. This can prevent the chance of a sub-optimal theme being presented to a user when they will accept multiple languages however prefer a language of an existing theme where language was not explicitly defined.

For example an English speaker may also understand French but not fluently. If a theme matches specifically on French and there are no other themes matching English the French theme will be presented even though the user has indicated a preference for English in their browser settings.

Theme A (No Theme/English Default)
Theme B (French)
** Theme C (English)

User A (Accept Languages: English, French)
User B (Accept Languages: French)
User C (Accept Languages: English)

Without the presence of “Theme C”, “User A” who prefers English but knows a little French is presented the French language version rather than the preferred English language version of the theme.

This occurs because ”Theme B” is more specific than “Theme A” as theme A provides no language requirement for matching.</td></tr>
<tr><td>Browser Type Match</td><td>Browser type matches on the User-Agent data provided by the users web browser. User Agent often provides information about the browser and sometimes also includes operating system, device type and even specific device models. The browser match field is matched as a case-insensitive substring to the User-Agent data provided by the web browser. Several examples of browser and device matching follow:

<table>
<tr><th>Match</th><th>Description</th></tr>
<tr><td>Windows</td><td>The client operating system is MS Windows</td></tr>
<tr><td>Windows NT 6.0</td><td>The client operating system is Windows Vista or Windows 2008</td></tr>
<tr><td>MSIE 7.0</td><td>The clients browser software is Internet explorer 7</td></tr>
<tr><td>Mac OS X</td><td>The clients operating system is Mac OS X</td></tr>
<tr><td>Opera</td><td>The clients browser software is Opera</td></tr>
<tr><td>Opera/9</td><td>The clients browser software is Opera 9.x</td></tr>
<tr><td>SymbianOS</td><td>The client is likely using a mobile device running the</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td>Symbian operating system.</td></tr>
<tr><td>Windows CE</td><td>The client is likely using a mobile device running the Windows mobile operating system.</td></tr>
<tr><td>Linux</td><td>The clients operating system is Linux</td></tr>
<tr><td>Firefox</td><td>The clients browser software is FireFox</td></tr>
<tr><td>IPhone</td><td>The client is an Apple mobile phone</td></tr>
<tr><td>BlackBerry</td><td>The client is a blackberry mobile phone</td></tr>
</table>
</td></tr>
<tr><td>Server root directory or URL</td><td>Specifies folder all content and related resources such as style sheets and images for the user facing login portal are located. All files must be located in the immediate directory referenced. A local directory path (ex ‘/usr/local/portal/html/tos’) or remote server URL (ex ‘http://myserver/amtos’) must be specified.

If a remote server is used content is downloaded by Air Marshal and presented to the user on behalf of the remote server much like a web proxy system. Use of a remote server can simplify integration with existing content management systems and allow multiple Air Marshal instances to source from a centralized location.

Please see the following section labeled Customizing for more information on required contents of the folder and information needed to customize aspects of the login portal.

Once a theme is saved the folder is checked for validity. If the check fails an error message explaining the failure is displayed in status field of the theme list. All errors must be addressed for themes to function properly. If there is a validation error for a local theme folder using a local pathname the theme is disabled and highlighted with a red background. The error must be corrected before the theme can be used. If the validation error occurs for a remote URL resource the error is presented but the theme remains active. This behavior minimizes the possibility of transient problems with a remote resource from being interpreted as a configuration failure.

If there is a validation problem and it has since been corrected simply choose a theme and save the theme to prompt the system to re-validate the configuration.</td></tr>
<tr><td>Content source extension</td><td>When server root directory is a URL the source extension field allows standard Air Marshal “.ptl” html files to be retrieved from the server using an alternate file extension such as “.html”, “.php”, “.asp”, “.jsp”..etc.

As an example assume server root folder is configured as follows:
http://myserver/amtos

Requests for the initial authorization file are normally directed to
http://myserver/amtos/authorize.ptl

By changing the source extension to “html” from the “ptl” default setting the Air Marshal requested file becomes:

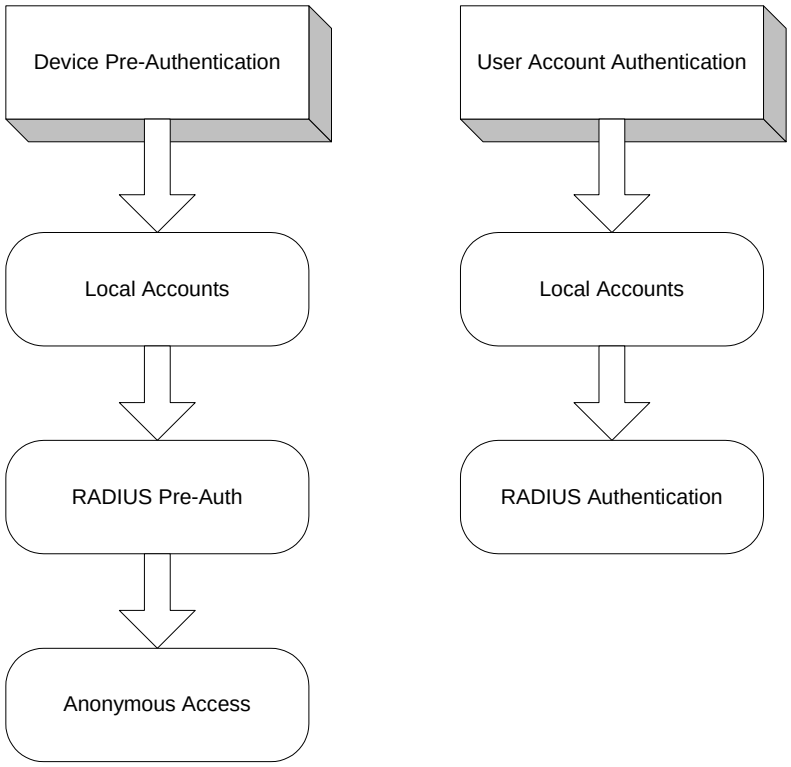
http://myserver/amtos/authorize.html

This allows remote system to be used without having to reconfigure extension associations within the external web system. All relative hyperlinks to html files within the folder must maintain the “ptl” extension when referencing each other regardless of the extension chosen.</td></tr>
</table>

	Incorrect: **<A HREF="moreinfo.html">Click here for more info</A>** Correct: **<A HREF="moreinfo.ptl">Click here for more info</A>**
Remote server content cache lifetime	When Server root directory field is a URL cache setting determines amount of time to cache a remote resource within Air Marshal such that Air Marshal answers subsequent requests for the same resource without having to query the remote web server. The cache can improve system performance and prevent short-term failures of the remote web server or network from affecting the login system. Clicking save changes in the Admin UI will trigger any cached content to immediately expire and new content downloaded from the remote web server as requested.
WISPr Location-ID	Location-ID is used in roaming environments to identify the physical hotspot location the end user is connecting. Location-ID is included in RADIUS Authentication and Accounting requests from Air Marshal.
WISPr Location Name	Location Name is used in roaming environments to identify the physical hotspot location the end user is connecting. Location-ID is included in RADIUS Authentication and Accounting requests from Air Marshal.
Comments	Optional informational only field to track notes and information related to the theme.

LOCAL ACCOUNT MANAGEMENT

While unsuitable for managing large numbers of accounts local account management provides for basic authentication services without the need for an external RADIUS server. Air Marshal provides two local authentication methods Anonymous Access that provides for guest access with daily usage limitations and Local Accounts, which provide login/password account, based management. The following diagram shows the order authentication methods are accessed during the client authentication process for both MAC based 'Pre-Authentication' and account authentication.

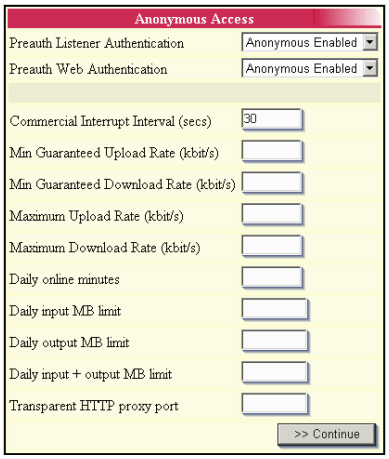


Accounting is handled the same way globally regardless of the authentication method used to authorize a client. If RADIUS Accounting is configured all authenticated sessions generate RADIUS accounting messages. If RADIUS Accounting is not configured accounting data is logged locally to 'Accounting log file' configured in the Debug & Logging menu.

Anonymous Access

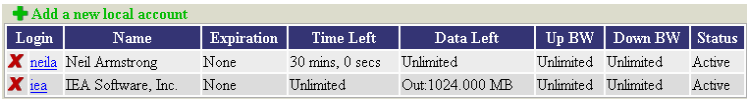
When enabled Anonymous Access provides guest access to the network with an optional set of limitations such as bandwidth and daily time or data restrictions. This is useful in situations where you may want to provide a certain level of free service such as one or two hours of service per day, provide advertising supported access or simply require users read and accept a terms of service agreement before gaining access to the network.

```
The 'Anonymous Access' authentication method must be enabled from the General Settings menu before this menu becomes visible.
```



Option	Description
Preauth Listener Authentication	When enabled preauth listeners (Outgoing requests to non HTTP based services) are allowed to use anonymous authentication to authenticate the users MAC after RADIUS and Local are attempted. If disabled anonymous access cannot be granted from a preauth listener.
Preauth Web Authentication	When enabled preauth web requests are allowed to use anonymous authentication to authenticate the users MAC after RADIUS and Local are attempted. If disabled anonymous access will not be granted to authenticate preauth web requests unless overridden by sending form field “anonkey” with a value of “1” during the preauth web request.
Commercial Interrupt Interval	When set commercial messages are displayed at the interval specified in seconds for the duration of the session. If left blank no commercial interruptions are performed.
Min Guaranteed Upload Rate	Minimum data rate guaranteed to each anonymous user. If not specified a minimum rate of 1/4th the maximum rate is used. If global Internet up/down bandwidth is not configured minimum guaranteed rate is not enforced.
Min Guaranteed Download Rate	Minimum data rate guaranteed to each anonymous user. If not specified a minimum rate of 1/4th the maximum rate is used. If global Internet up/down bandwidth is not configured minimum guaranteed rate is not enforced.
Maximum Upload Rate	Maximum enforced data upload rate in kbits per second.
Maximum Download Rate	Maximum enforced data download rate in kbits per second.
Daily online minutes	Number of minutes the client is allowed to login per day. Usage allowances are reset daily after midnight.
Daily input MB limit	Number of megabytes the client is allowed to upload per day. Usage allowances are reset daily after midnight.
Daily output MB limit	Number of megabytes the client is allowed to download per day. Usage allowances are reset daily after midnight.
Daily input + output MB limit	Number of megabytes the client is allowed to download and upload per day. Usage allowances are reset daily after midnight.
Transparent HTTP proxy port	Enables normal HTTP traffic for the users session to be redirected to a transparent HTTP proxy server installed on the Air Marshal server. The value of this attribute corresponds to the TCP port the transparent proxy is listening.

Local Accounts

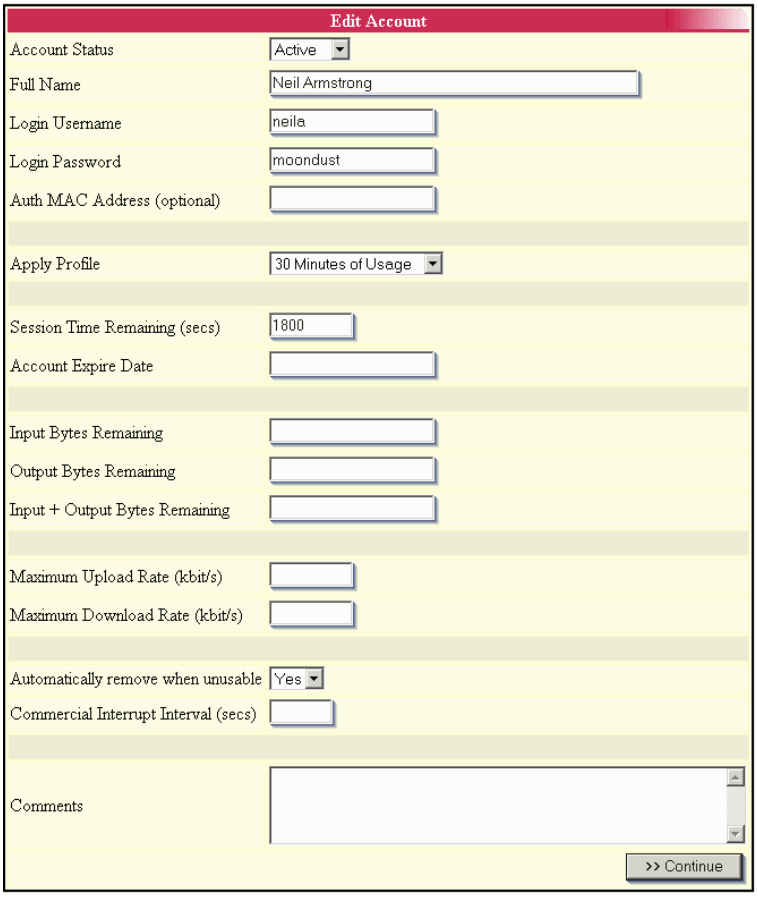


Local accounts provide basic client authentication based upon network address or username and password. In addition Air Marshals account profile system enables simplified configuration of accounts by applying standard sets of stored profiles. Profiles enable common limits such as account expiration and data usage restrictions.

To add or manage existing accounts choose the Local Accounts menu option. To add new accounts select the 'Add new local account' link. To make changes to an existing account click the login name from the listing or click the red 'x' to remove the account. All changes to account information take effect instantly.

The 'Local Accounts' menu will only appear after Air Marshal has been started successfully and the Local Accounts authentication method is enabled from the General Settings menu.

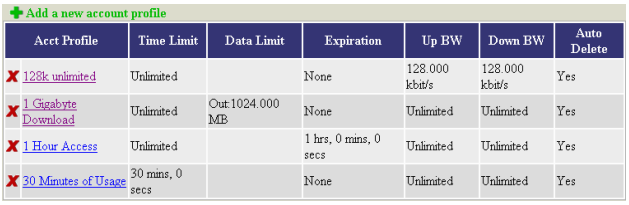
Local Accounts are not intended to manage large numbers of accounts. A centralized RADIUS server and management platform such as Emerald should be considered if there is a need to manage a large list of subscribers.

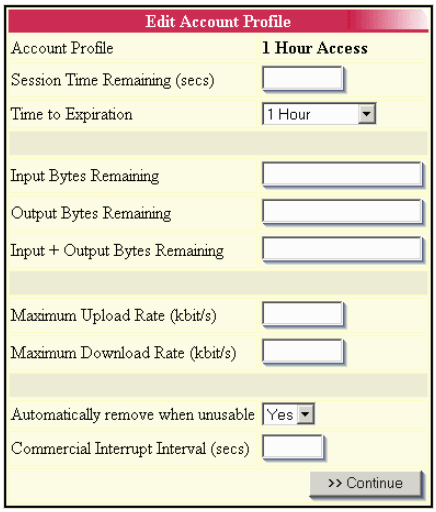


Option	Description
Account Status	Sets the active status of the account. If Active the account subject to any additional restrictions is usable. If Inactive the account is not able to authenticate.
Full Name	The full name of the user assigned to the account.
Login Username	The login username of the user assigned to this account. If you are doing client device based authentication the clients MAC address should be entered here in lieu of username.
Login Password	The login password associated with this account. Note: If device based authentication is performed the login password field is unused.
Auth MAC Address	When set the user logging on must have a client device with the same MAC address listed in this field. If they do not match the client logon attempt fails.
Apply Profile	Applies a stored configuration profile to the account. Apply profile is only visible if any Account Profiles have been configured. When a profile is applied its configuration completely replaces all values except for the following account specific fields: Full Name, Login Username, Login Password, Auth MAC Address and Comments.
Session Time Remaining	The total number of seconds of online time remaining before the account is no longer usable. If no value is specified the account has no session time limit.
Account Expire Date	A set date after which the account becomes unusable. Users logging in prior to this date will be disconnected as the date is reached. If no value is specified the account never expires.
Input Bytes Remaining	Number of bytes the user can upload before their session is disconnected and the account becomes unusable. If no value is specified this restriction does not apply.
Output Bytes Remaining	Number of bytes the user can download before their session is disconnected and the account becomes unusable. If no value is specified this restriction does not apply.
Input + Output Bytes Remaining	Combined number of bytes the user can upload and download before their session is disconnected and the account becomes unusable. If no value is specified this restriction does not apply.
Maximum Upload Rate	Applies an upload bandwidth rate restriction to the user in kbits per second. If blank no artificial bandwidth limits are applied.
Maximum Download Rate	Applies a download bandwidth rate restriction to the user in kbits per second. If blank no artificial bandwidth limits are applied.
Automatically remove when unusable	When set 'Yes' and the account is unusable for any reason such as being inactive, expired or exceeding a data or time limitation the account is automatically deleted after midnight. When set 'No' the unusable account remains in the local account listing indefinitely.
Commercial Interrupt Interval	When set commercial messages are displayed at the interval specified in seconds for the duration of the session. If left blank no commercial interruptions are performed.
Transparent HTTP proxy port	Enables normal HTTP traffic for the users session to be redirected to a transparent HTTP proxy server installed on the Air Marshal server. The value of this attribute corresponds to the TCP port the transparent proxy is listening.
Comments	Notes or special instructions related to the account may be entered here.

Account Profiles

Profiles are applied to new or existing local accounts through the Local Accounts menu. The use of profiles enables common limits such as account expiration and data usage restrictions to be applied uniformly to an account.





Option	Description
Account Profile	Name describing the purpose of the profile. The profile name is listed in the account profile selection list within the Local Accounts menu.
Session Time Remaining	The total number of seconds of online time remaining before the account is no longer usable. If no value is specified the account has no session time limit.
Time to Expiration	Amount of time starting from when the profile is assigned to . If no value is specified the account never expires.
Input Bytes Remaining	Number of bytes the user can upload before their session is disconnected and the account becomes unusable. If no value is specified this restriction does not apply.
Output Bytes Remaining	Number of bytes the user can download before their session is disconnected and the account becomes unusable. If no value is specified this restriction does not apply.
Input + Output Bytes Remaining	Combined number of bytes the user can upload and download before their session is disconnected and the account becomes unusable. If no value is specified this restriction does not apply.
Maximum Upload Rate	Applies an upload bandwidth rate restriction to the user in kbits per second. If blank no artificial bandwidth limits are applied.
Maximum Download Rate	Applies a download bandwidth rate restriction to the user in kbits per second. If blank no artificial bandwidth limits are applied.
Automatically remove when unusable	When set 'Yes' and the account is unusable for any reason such as being inactive, expired or exceeding a data or time limitation the account is automatically deleted after midnight. When set 'No' the unusable account remains in the local account listing indefinitely.
Transparent HTTP proxy port	Enables normal HTTP traffic for the users session to be redirected to a transparent HTTP proxy server installed on the Air Marshal server. The value of this attribute corresponds to the TCP port the transparent proxy is listening.
Commercial Interrupt Interval	When set commercial messages are displayed at the interval specified in seconds for the duration of the session. If left blank no commercial interruptions are

	performed.

CUSTOMIZING

Air Marshal communicates with the user through a configurable set of html files. Files included with the default server installation provide general functionality intended to be used as a template for creating a customized user experience to match the venue of your clients. Two separate user interface examples are included with Air Marshal. Either can be customized to provide the branding and features necessary. See General Settings / 'Server root directory' for more information on each.

HTML

The files in the table below make up the user interface. Air Marshal sends each file to the user where appropriate depending on the current state of their session. You cannot reference any files that do not have the extensions .gif, .jpg, .png, .css, .js or .ptl**.** If content with any of these extensions is located on a remote web server URL configured within a Theme it is downloaded from the remote server and treated as if it were a local file.

Files with the .ptl extension are HTML files supporting simple variable substitutions to allow status information to be presented to the user and can typically be manipulated by any html editing software.

```
Air Marshal will not display files with the extension of .htm or .html.  The
.ptl extension is necessary to mitigate the possibility of name collisions
with third party web sites captured and redirected to the Air Marshal
interface.
```

HTML file	Description
ack.ptl	Displayed after a successful login. Indicates the user logged in and displays information about the session.
nak.ptl	Displayed after an unsuccessful login. Usually shows a message to try again ($replymsg) and redisplays the login page.
login.ptl	Displays main login form collecting username and password variables. Note: the form variable 'authkey' must be sent with username and password to successfully authenticate. The value of authorization key is available via the $srcauthkey variable.
logout.ptl	Displayed after the users session has closed
error.ptl	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.ptl	After successfully logging in this displays information about the users session, how much time they've used so far, time remaining…etc.
authorize.ptl	Displays a message to get authorization for the authentication process such as agreeing to terms of service or watching a commercial advertisement before directing the user to login.ptl /w the authorization key variable $srcauthkey
interrupt.ptl	Commercial message to be displayed when a user's session is commercially interrupted. This page can link to others to display a series of advertising messages. Commercial interruption is completed when the form variable authkey is posted to a subsequent page

	with the contents of the $srcauthkey variable.

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	Ping script
$error	Displays the contents of any error messages	Yes	No
$login	Username form variable passed to Air Marshal	N/A	N/A
$password	Password form variable passed to Air Marshal	N/A	N/A
$referer	Referrer form variable passed to Air Marshal.	N/A	N/A
$replymsg	Auth response message	Yes	No
$user	Name of logged in user	Yes	No
$sessionid	Unique ID of current session	Yes	No
$timeleft	Amount of time remaining or 'Unlimited'.	Yes	No
$inleft	Count of incoming data remaining before session is terminated	Yes	No
$outleft	Count of outgoing data remaining before session is terminated	Yes	No
$dataleft	Count of the sum of incoming + outgoing data remaining before session is terminated	Yes	No
$inused	Count of incoming data used in current session	Yes	No
$outused	Count of outgoing data used in current session	Yes	No
$dataused	Count of incoming + outgoing data used in current session	Yes	No
$maxup	Maximum upload rate in bits per second	Yes	No
$maxkup	Maximum upload rate in kbits per second	Yes	No
$maxdown	Maximum download rate in bits per second	Yes	No
$maxkdown	Maximum download rate in kbits per second	Yes	No
$idletimeout	Displays the account's idle timeout setting	Yes	No
$timeon	Amount of time spent online so far	Yes	No
$referer	Original URL client was initially redirected from	Yes	No
$authkey	Represents the current value of the $authkey form variable. The current authorization key must be obtained from $srcauthkey	Yes	No
$srcauthkey	Contains current session authorization key that must be sent as the form variable 'authkey' to authenticate.	Yes	No
$var1	Used to pass information between html forms	Yes	No
$var2	Used to pass information between html forms		
$ip	IP Address of connected client	Yes	Yes
$mac	MAC Address of connected client	Yes	Yes
$mode	Session tracking 1=Layer2, 2=Layer3	No	Yes

$serverurl	URL of the server	Yes	No
$redirecturl	Redirect URL	Yes	No
$authmethod	Password authentication method – 1=PAP, 2=CHAP	Yes	No
$framedip	Contains assigned Framed-IP-Address from RADIUS access accept	Yes	No
$theme	Name of theme used to present login UI to the end user.	Yes	No
$locationid	WISPr Location ID	Yes	No
$locationname	WISPr Location Name	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

- 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 files a required package may need to be installed.

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.

Solution #3 Make sure the RADIUS shared secrets between RADIUS server and authentication gateway exactly match.

NAT/Routing (Linux)

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, VoIP, VPNs and some multi-player games to work through NAT. Air Marshal activates these modules automatically to provide maximum compatibility. See your operating system documentation for more information on NAT (IP Masquerade) and its limitations.

Misc

Problem. Entries in the who's online display appear with a red background.

Solution. This can happen when the system calls to enable a session fail. Enable full debug to isolate the cause of the problem.

RADIUS ATTRIBUTES

Authentication

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

RADIUS Vendor	RADIUS Attribute	Direction	Description
Standard	User-Name	Access-Request	This Attribute indicates the name of the user to be authenticated.
Standard	User-Password	Access-Request	PAP Password
Standard	CHAP-Password	Access-Request	CHAP Password
Standard	CHAP-Challenge	Access-Request	CHAP Challenge string
Standard	Framed-IP-Address	Access-Request	Reflects the authenticating clients IP Address.
Standard	Calling-Station-Id	Access-Request	(Caller-ID) If available the authenticating clients MAC address is sent via this attribute in hexadecimal form without a byte delimiter.
Standard	Acct-Session-Id	Access-Request	Used to uniquely identify each session and match start and stop records.
Standard	NAS-Port	Access-Request	This attribute indicates the virtual port number the user has attached. Port numbers are allocated out of a sequential pool to maximize the ability to detect gaps in available accounting data. This attribute is sent when Network Options / "Per session NAT port allocation" is set to "Dynamic".
Standard	NAS-Port-Id	Access-Request	This attribute indicates the range of source ports for TCP and UDP allocated to the session when used in a shared NAT environment. This value is

			formatted as "1024-1034" specifying the starting and ending TCP/UDP source port range allocated to the session. This attribute is sent when Network Options / "Per session NAT port allocation" is set to a value other than "Dynamic".
Standard	NAS-Port-Type	Access-Request	Provides information regarding type of network access technology the user is attached. The default value is “Virtual” and may be changed via RADIUS accounting menu.
Standard	Service-Type	Access-Request	Provides information regarding type of network service the user is to be provided. The default value is “Framed-User” and may be changed via RADIUS accounting menu.
WISPr	Location-ID	Access-Request	Hotspot location identifier. Determined via the WISPr Location-ID option within a theme or the Radius Accounting menu.
WISPr	Location-Name	Access-Request	Hotspot location name. Determined via the WISPr Location Name option within a theme or the Radius Accounting menu.
Standard	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
Standard	Framed-IP-Address	Access-Accept	Used to setup a one-to-one NAT association of the specified Framed-IP-Address to the users internal address. To be honored the Framed-IP-Address configuration option in the RADIUS Auth menu must be enabled.
Standard	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 MAC address tracking and the active ping script if one was defined for this session. Currently idle timeout is only supported when Layer 2 session tracking mode is enabled. Note: Due to the popularity of application level keepalives in many common applications enforcement of Idle-Timeout should be considered unreliable.
Standard	Class	Access-Accept	Data received from this attribute during an Access-Accept is sent out in associated accounting – start/stop requests.
Standard	Filter-Id	Access-Accept	Used to pass parameters to Air Marshal to control authorization features. Values sent must be in the form parametername=parametervalue (Named values contain the attribute name FILTERAVP)
Standard	Tunnel-Password	Access-Accept	Used to pass parameters to Air Marshal to control authorization features. Values sent must be in the form parametername=parametervalue (Named values contain the attribute name FILTERAVP)

Standard	Acct-Interim-Interval	Access-Accept	If specified RADIUS interim accounting updates are issued for this session at the set interval in seconds. If not specified interim accounting is controlled from the Interim update interval option of the RADIUS Accounting menu.
N/A	FILTERAVP:htmlack	Access-Accept	If specified filename is sent in place of ack.ptl after successful authentication.
N/A	FILTERAVP:htmlstatus	Access-Accept	If specified filename is sent in place of status.ptl to display session status.
N/A	FILTERAVP:mirror	Access-Accept	If specified with a value of 'local' (mirror=local) client data mirroring copies all data traffic for a user session authenticated via RADIUS to ethereal/wireshark compatible capture files stored in the /usr/local/portal/mirror folder. Files are created in roughly 20 megabyte chunks in the form: user_session_YYYYMMDD_HHMMSS_seq.pcap Where user is the logged on username or MAC/IP if preauth is used. Session is the users session identifier (Acct-Session-ID in RADIUS Accounting Messages) Time fields always reflect the starting time of the user session. Seq is the sequence number of the capture file. Starting at 1 and incrementing for each ~20MB chunk each time a new file is created during the session. Note for any given session only the sequence field is changed. Session id and time fields remain constant for the duration of the session.
N/A	FILTERAVP:whomsg	Access-Accept	If specified value contains a short message appearing in the Air Marshal who's online listing for the current session.
N/A	FILTERAVP:extcmd	Access-Accept	Used to provide for custom provisioning when opening and closing a session. During action=sesopen and action=sesclose this value is passed as the parameter extcmd to portalshell. To be effective customizations must be made to the shellkey to provide for custom action. The value is limited to 63 characters and must contain only alphanumeric characters or '.'.
WISPr	Redirection-URL	Access-Accept	URL Presented to the user after they have successfully authenticated. If this attribute is not specified the user is redirected to the web site they originally intended to go to upon successful authentication.
WISPr	Bandwidth-Max-Up	Access-Accept	Maximum upload bandwidth allocated to the user in bits-per-second. Note: 128000bps = 128kbps

WISPr	Bandwidth-Max-Down	Access-Accept	Maximum download bandwidth allocated to the user in bits-per-second. Note: 128000bps = 128kbps
WISPr	Bandwidth-Min-Up	Access-Accept	Minimum guaranteed upload bandwidth allocated to the user in bits-per-second. If additional bandwidth is available the user will be provided with additional bandwidth limited to Bandwidth-Max-Up. If not specified Bandwidth-Max-Up is the minimum bandwidth. Note: 128000bps = 128kbps
WISPr	Bandwidth-Min-Down	Access-Accept	Minimum guaranteed download bandwidth allocated to the user in bits-per-second. If additional bandwidth is available the user will be provided with additional bandwidth limited to Bandwidth-Max-Down. If not specified Bandwidth-Max-Down is the minimum bandwidth. Note: 128000bps = 128kbps
WISPr	Session-Input-Octets	Access-Accept	Maximum upload byte count before the session is disconnected.
WISPr	Session-Input-Gigawords	Access-Accept	Maximum upload byte count before the session is disconnected. (Gigawords * 2^32)
WISPr	Session-Output-Octets	Access-Accept	Maximum download byte count before the session is disconnected.
WISPr	Session-Output-Gigawords	Access-Accept	Maximum download byte count before the session is disconnected. (Gigawords * 2^32)
WISPr	Session-Octets	Access-Accept	Maximum combined upload and download byte count before the session is disconnected.
WISPr	Session-Gigawords	Access-Accept	Maximum combined upload and download byte count before the session is disconnected. (Gigawords * 2^32)
IEA Software	AM-Interrupt-HTMLFile	Access-Accept	Local name of file displayed when commercial session interruption is in effect. If attribute is not specified the default file displayed is interrupt.ptl
IEA Software	AM-Interrupt-Interval	Access-Accept	Commercial interruption interval in seconds. If specified the session is interrupted at the interval specified to display commercial messages. If not specified no commercial interruption is done.
IEA Software	AM-Interrupt-Timeout	Access-Accept	Sets the length of time in seconds since the start of a commercial interruption to wait for the commercial to be acknowledged before the session is disconnected. If not specified the Commercial interrupt timeout setting in the Session Settings menu is used.
IEA Software	AM-Status-HTMLFile	Access-Accept	If sent an alternate session status file can be presented to the user displaying the current status of their session such as time used, time left, data left..etc. If not specified the status file status.ptl is sent to the user.
IEA Software	AM-ACK-HTMLFile	Access-Accept	If specified filename is sent in place of ack.ptl after successful authentication.
IEA	AM-NAK-HTMLFile	Access-Reject	If specified filename is sent in place of nak.ptl after

Software			failed auth attempt.
IEA Software	AM-Bandwidth-Pool	Access-Accept	Named bandwidth pool to be associated with the user session. Bandwidth pools constrain a subset of sessions to a shared data limit. When specified AM-Bandwidth-Pool-Max-Up and or AM-Bandwidth-Pool-Max-Down must also be specified to define the pools data rate.
IEA Software	AM-Bandwidth-Pool-Max-Up	Access-Accept	Total upload bandwidth limit applicable across all sessions having the same AM-Bandwidth-Pool. This value must be set consistently per unique pool label AM-Bandwidth-Pool. If a new session is started with a different bandwidth pool allocation from previous sessions already sharing the same bandwidth pool label the bandwidth allocation is updated and all current sessions are updated with the new limit.
IEA Software	AM-Bandwidth-Pool-Max-Down	Access-Accept	Total download bandwidth limit applicable across all sessions on the same managed subnet interface having the same AM-Bandwidth-Pool. This value must be set consistently per unique pool label AM-Bandwidth-Pool. If a new session is started with a different bandwidth pool allocation from previous sessions already sharing the same bandwidth pool label the bandwidth allocation is updated and all current sessions are updated with the new limit.
IEA Software	AM-Mirroring	Access-Accept	A value of 1 indicates local client data mirroring is enabled. For more information on data mirroring see attribute FILTERAVP:mirror above.
IEA Software	AM-HTTP-Proxy-Port	Access-Accept	Enables normal HTTP traffic for the users session to be redirected to a transparent HTTP proxy server installed on the Air Marshal server. The value of this attribute corresponds to the TCP port the transparent proxy is listening.
Ascend	Data-Filter	Access-Accept	Ascend Binary data filter attribute used to filter a client's access to the network. Binary data filters are typically used to enforce limits on SMTP server access in roaming environments to cut down on spam. Note: Air Marshal currently supports only IP based filters, different destination and source ports can't be specified in the same rule, "Established" keyword is not supported or comparison operations other than equal.

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, 3=Interim, 7=Acct On, 8=Acct Off
Acct-Delay-Time	This attribute indicates how many seconds the client has been trying to send this record to the RADIUS accounting server, delay time is subtracted from the time of arrival on the server to determine 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	Used to uniquely identify each session and 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 the user has attached. Port numbers are allocated out of a sequential pool to maximize the ability to detect gaps in available accounting data. This attribute is sent when Network Options / "Per session NAT port allocation" is set to "Dynamic".
NAS-Port-Id	This attribute indicates the range of source ports for TCP and UDP allocated to the session when used in a shared NAT environment. This value is formatted as "1024-1034" specifying the starting and ending TCP/UDP source port range allocated to the session. This attribute is sent when Network Options / "Per session NAT port allocation" is set to a value other than "Dynamic".
NAS-Port-Type	Provides information regarding type of network access technology the user is attached. The default value is “Virtual” and may be changed via RADIUS accounting menu.

Service-Type	Provides information regarding type of network access technology the user is attached. The default value is "Framed-User" and may be changed via RADIUS accounting menu.
Connect-Info	When a theme is used this attribute indicates the name of the theme matched to the user. When no theme is matched the attribute indicates the network interface the client was attached.
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.
Framed-IP-Address	IP Address assigned to the client.
WISPr-Location-ID	Hotspot location identifier. Determined via the WISPr Location-ID option within a theme or the Radius Accounting menu.
WISPR-Location Name	Hotspot location name. Determined via the WISPr Location Name option within a theme or the Radius Accounting menu.

Disconnect

The following attributes may be sent in a Disconnect-Request. If an attribute is included in a disconnect request its value must exactly match that of the session even if it is not a required attribute.

RADIUS Attribute	Required	Description
Acct-Session-Id	Yes	Used to uniquely identify each session and match start and stop records.
NAS-Port	No	This attribute indicates the virtual port number the user has attached. Port numbers are allocated out of a sequential pool to maximize the ability to detect gaps in available accounting data.
NAS-Port-Id	No	This attribute indicates the range of source ports for TCP and UDP allocated to the session when used in a shared NAT environment. This value is formatted as "1024-1034" specifying the starting and ending TCP/UDP source port range allocated to the session.
User-Name	No	This Attribute indicates the name of the user to be authenticated.
Framed-IP-Address	No	IP Address assigned to the client.
Calling-Station-Id	No	(Caller ID) MAC Address of the client, if available.

Change of Authorization (CoA)

To change the authorization parameters of an active session a CoA request is issued containing session identifying attributes per Disconnect in the table above followed by a list of changed authorization attributes from the Authentication table above.

The following authorization attribute usage limits apply to CoA requests. To effect change of the session parameters listed below CoA cannot be used. The session must be disconnect and reestablished.

- Only attributes from Authentication table above with a direction of "Access-Accept" may be used.
- No FILTERAVP attribute may be specified using either Framed-Filter or Tunnel-Password.

- Ascend data filter changes are unsupported
- Data mirroring changes are unsupported
- Framed-IP-Address is a session identifying attribute and cannot also be used in the context of changing one-to-one NAT associations.

ACKNOWLEDGEMENTS

TLS features based on the OpenSSL project

MD5 compliments of RSA Data Security, Inc

MD5 JavaScript implementation by David West

Air Marshal Auth Gateway Programming & Documentation by IEA Software, Inc