CMS User Manual

For General Operation

Quick Reference

1. **Who is this Manual For?**
   This manual covers general accessibility and functionality for the Mako System. However, there may be individual functions that are disabled or unavailable. This is likely because the user:
   a. does not have clearance to use the function.
   b. has set options that make related functions redundant.
   c. has not selected a Mako to configure.
2. **What Isn't Covered**
   This is a guideline for using the Mako CMS to configure and manage your Mako in a conventional environment. The following features, while accessible to many users, are covered in different manuals:
   a. Reporting
   b. Deployment
   c. Guardian
   d. Mako Mail
3. **CMS navigation**
   There are different ways to navigate to certain pages, but the left-side tab-strip is common to all. This manual uses the following shorthand for following the sub-tabs:

   Main Tab > Sub-tab(s) > Final Page
4. **Note Icons**

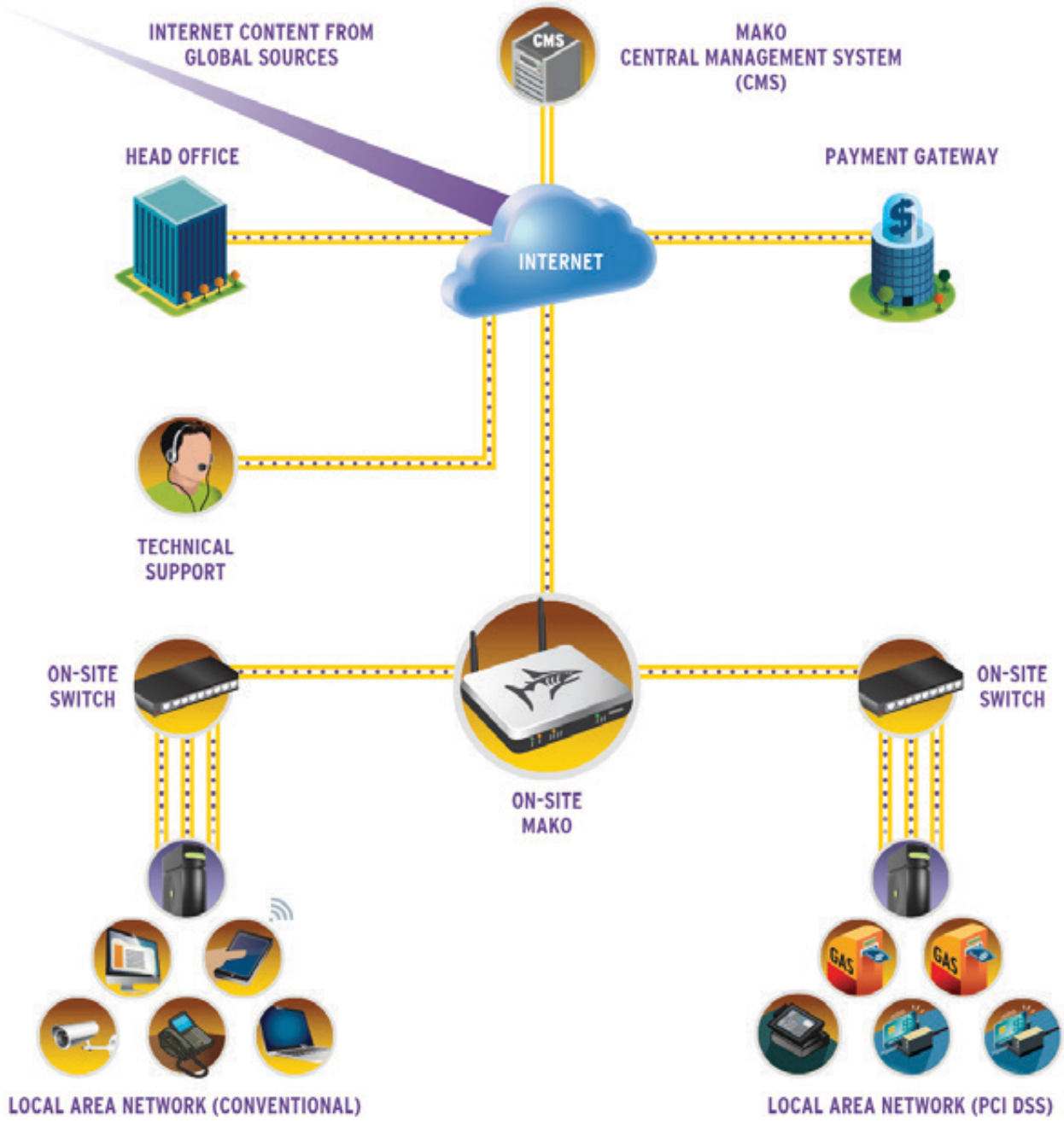
Note: Usually not critical for the normal operation of the system.

Warning: The note requires your attention and will affect the way you and other approved users will use your system.

5. **Cookies**
   Cookies must be enabled when using the CMS.

This reference is an overview. Read this guide fully for details.

The Mako System: Overview



The Mako System offers a cloud-managed, turnkey solution to create and manage broadband networks for small sites.

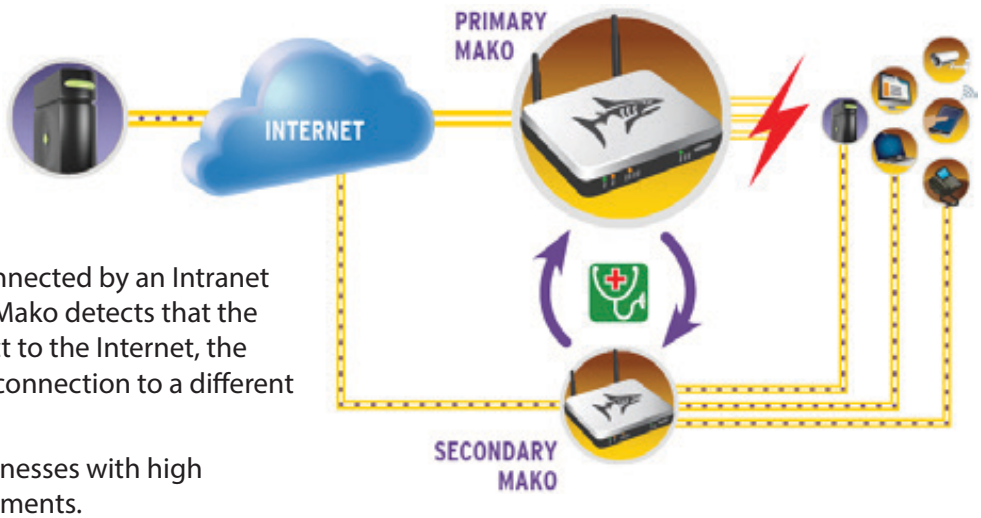
The Mako System provides businesses with a standard of information security that meets the **Payment Card Industry Data Security Standard (PCI DSS)**.

Your Mako is managed remotely by Mako Networks via a web server, using your Internet connection and the **Central Management System (CMS)**. The CMS uses a web browser for personal configuration and reporting.

Your Mako, CMS and the hosted management servers are referred to as the **Mako System.**

The Mako System: Failover

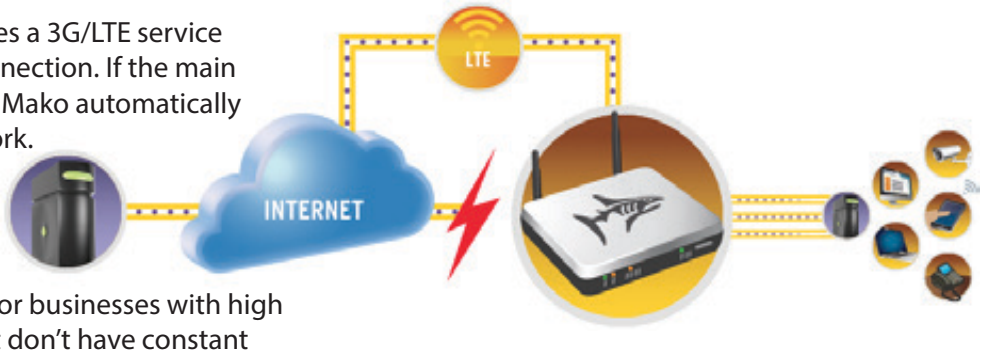
Dual Mako Failover



A location has two Makos connected by an Intranet 'heartbeat'. If the Secondary Mako detects that the Primary Mako cannot connect to the Internet, the Secondary takes over with a connection to a different Internet service.

Dual Mako Failover is for businesses with high availability and traffic requirements.

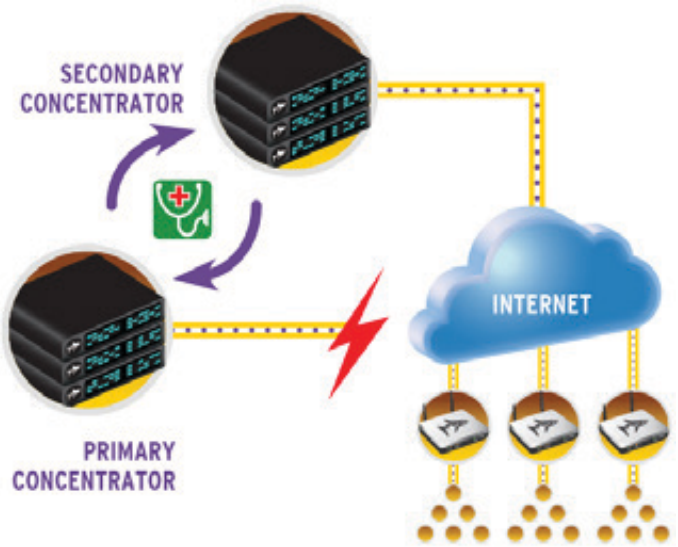
Cellular Failover



A cellular-equipped Mako uses a 3G/LTE service as an alternative Internet connection. If the main Internet connection fails, the Mako automatically re-connects over a cell network.

Cellular Failover is generally for businesses with high availability requirements, but don't have constant high traffic demands. A common use is for retailers over holiday periods. During local outages an alternate Internet connection mitigates loss of sales.

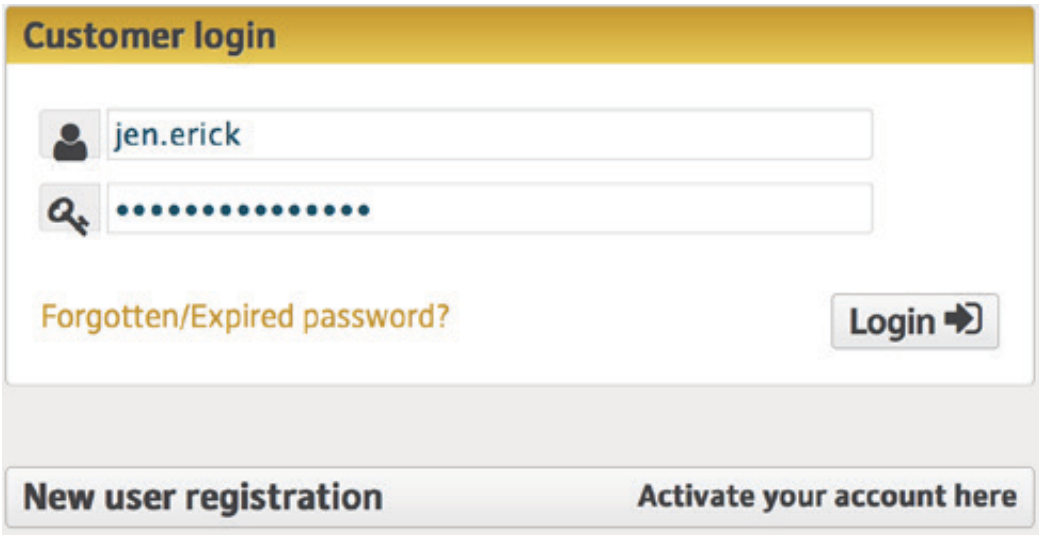
Geographic/Data Center Failover



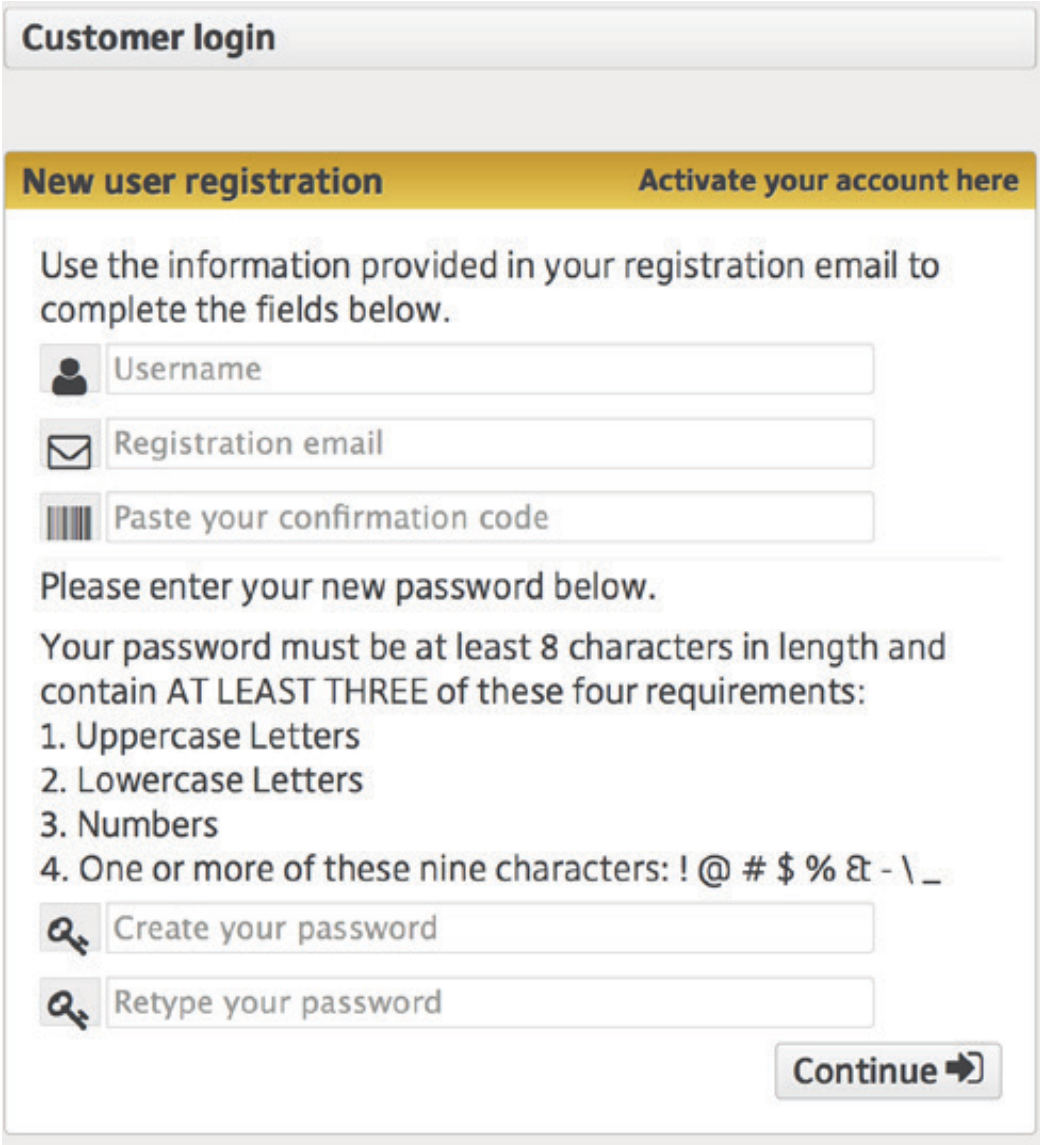
The CMS is run by a series of concentrators – servers geared for running thousands of private networks. If a concentrator fails, the entire network management is transferred to another concentrator.

Geographic Failover is for enterprise-level businesses with high availability requirements.

Contents



1.2 LOGIN



1.3 FORGOTTEN/EXPIRED PASSWORDS

1 Registration & Login

When your account is set up, the CMS emails you your accounts details, along with a link to log you into your network. [i]

Registration is a one-time process that activates the account created for you by your reseller on the CMS.

You'll be sent an email with a link. New user registration is done when you follow the link, either by clicking it or pasting the link into your web browser's address bar.

1.1 Home > New User Registration

- Enter the appropriate details. [ii]

1.2 Login

- Click the link, or open your Web browser and navigate to your Mako Management CMS.
- Click the Customer Login button, top right of the page. If you're operating in a PCI environment you will need to provide the reCAPTCHA login details.
- If your login is incorrect you'll be asked to re-enter your information. [iii]

If your system has a PCI template, it has the ability to handle 2 sets of internet traffic: PCI-compliant (usually for credit card transactions), and non-PCI-compliant (for general internet traffic).

If you don't have a PCI template, you have two still have two separate traffic routes with our entry-level appliances. For example, one could be used for a public, general access pipe (often called a DMZ) for a web server. Our higher capacity appliances provide up to 4 LANs simultaneously. [iv]

1.3 Forgotten/Expired Passwords

If you forget your password, or your password has expired:

- In the Customer Login page click **Forgotten/Expired password?**
- Your email notification or reseller will supply you with the necessary steps to re-enter your system.

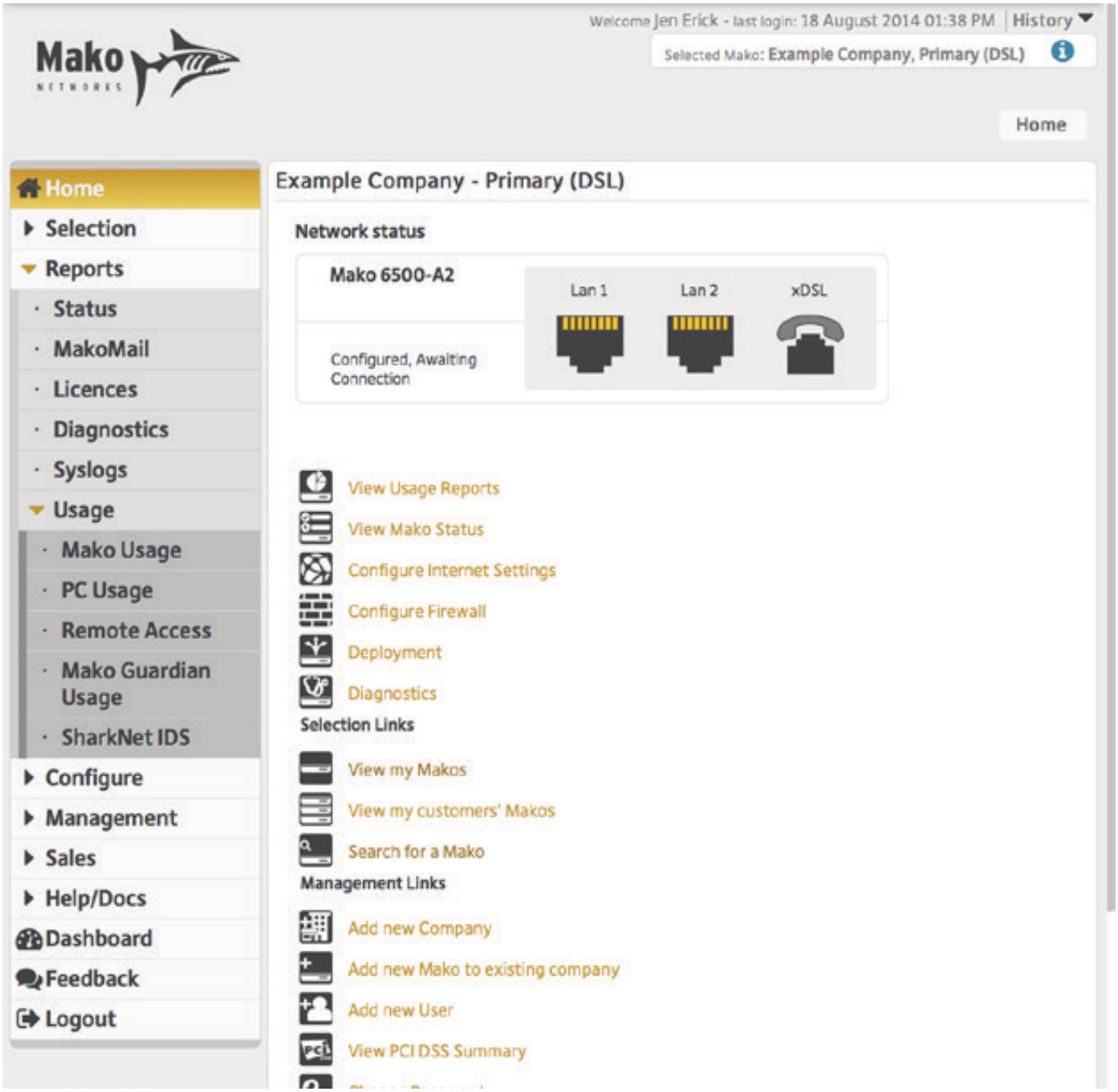
---

[i] Your browser must accept cookies and must have JavaScript enabled to access the CMS website. These properties are set in your browser preferences and are normally enabled by default.

[ii] You will be asked to read and acknowledge the End User License Agreement (EULA) before you can start using your system.

[iii] Logins and passwords are your last line of protection for ensuring your system remains robust. Never give you login or password out to anyone else.

[iv] While you may run separate LANs, each Mako runs on only one CMS. Only one login/password is assigned to a user, but one user may be set up to manage several Makos. PCI-compliant traffic requires you to change your password every 90 days. If you have configured a non-PCI network then security is more forgiving, allowing you to maintain or change your password as you see fit.



2.1 THE LEFT MAIN MENU

2 Home

The Home page is the starting point for administration and monitoring of your Makos and users.

2.1 The Left Main Menu

- **Reveal triangles ( ) show more options are within that menu.** Dark triangles indicate collapsed options, coloured triangles indicate revealed options.
- **Dotted menu options indicate no sub-menus are within this option.**

2.2 Status Icons

Your system uses a small set of status icons to present instruction and data consistently:

Help

Information hover-text

Warning/Important

Allow traffic/Active

Deny Traffic

Default Mode

Edit DHCP settings

Awaiting Connection

2.3 The Header Bar

The header gives you an immediate overview of your account, access history and general info.

The top line gives you the user access details, time and company you're operating under for this session.

Also here is:

"Name" The name of the selected Mako.

Information. Click this for this Mako's configuration profile.

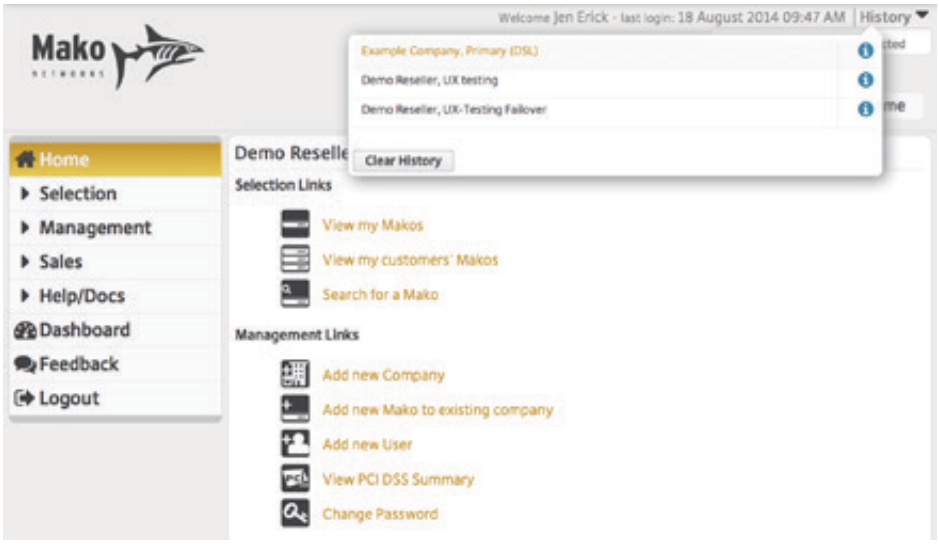
2.4 The Body Section

2.4.1 Port Widget

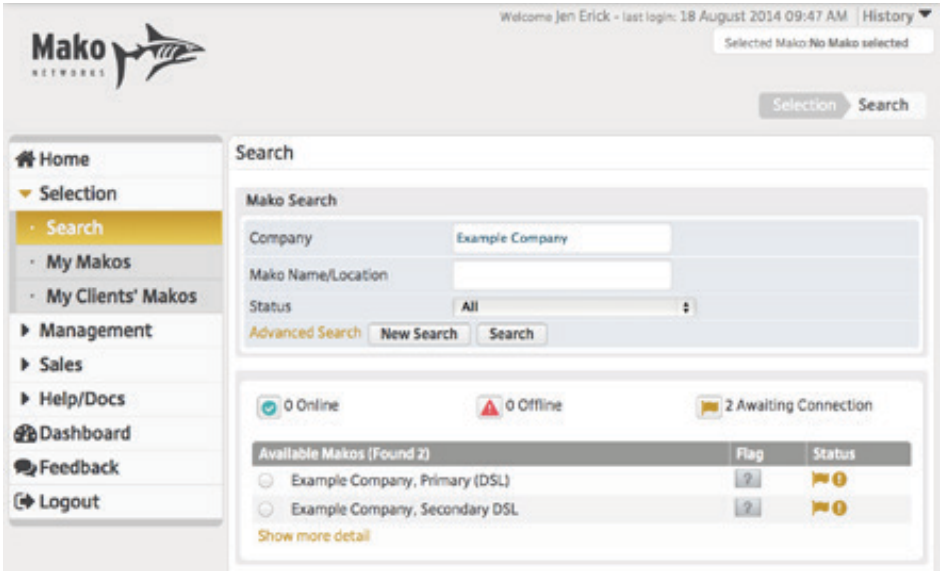
The topmost diagram illustrates which LAN ports have been configured for use. It's a quick overview of which ports are in use over what IP, if Failover is enabled and to which Mako, and if SIM cards are present.

2.4.2 Page Body

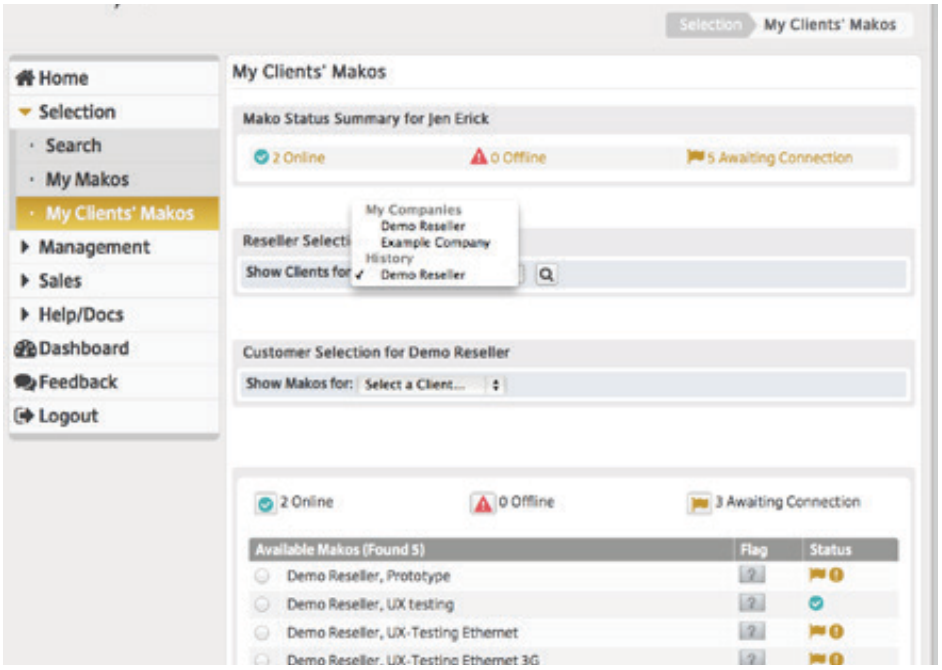
The Body of a page either contains a list of shortcuts to pages nested in the left navigation menu, or the settings interface for a page.



3.1 HISTORY SHORTCUT



3.2 > SEARCH



3.4 > MY CLIENT'S MAKOS

3 Selection

The Selection menu allows you to select an individual Mako in your network and interrogate it. [i]

3.1 History Shortcut

Use the **History** shortcut, top right of the CMS screen, for a recently selected Mako.

3.2 › Search

- Enter a company and/or name location field. Click Search.
- Click your target Mako's radio button from this list. The default selection will be the topmost Mako.

3.2.1 Advanced Search › Enter your ID

Your network can be searched using a Mako ID.

3.3 › My Makos

- Select a Mako's radio button. The header will update.

3.3.1 Show more detail

This link adds two more columns to the table: Usage (in MB), and Current IP.

3.4 › My Client's Makos

- **Select a Client...** from the drop-down menu.
- Select a Mako's radio button. Following any one of the methods above, you should have a selection of Makos to choose from, and:
- At the top of the page, your login, location, time and Mako details appear in the Header bar.
- The Mako's Status, Info and History shortcuts also appear in the Header bar. Several features will appear in the main menu. [ii]

3.4.1 List Filtering

To filter your results by Online, Offline or Awaiting Connection status categories:

- In the Mako Status Summary above the list, click , or to filter the results by connection status.

3.4.2 Seeing a Mako's Information Window

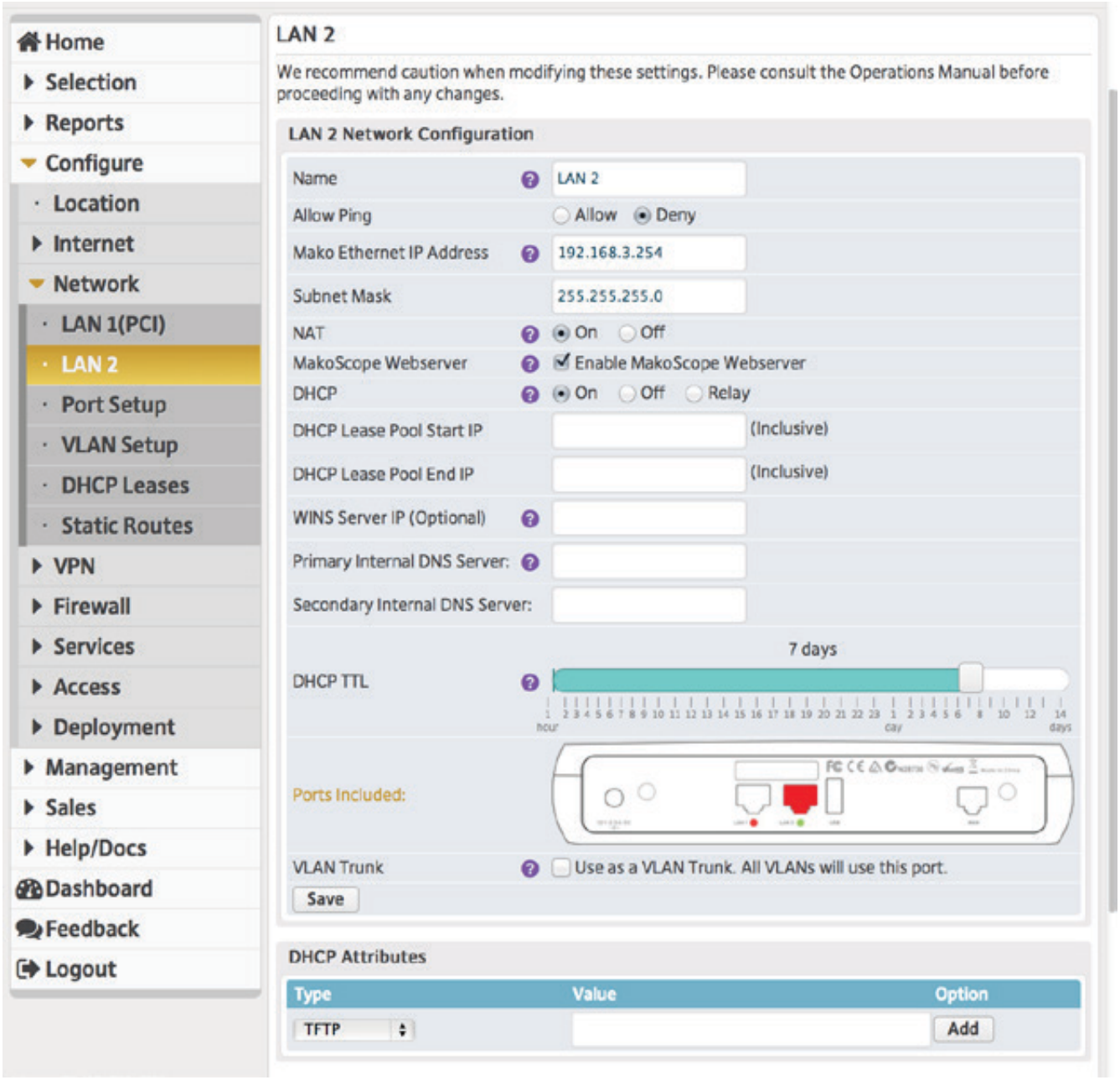
- Click on the icon in the header bar, OR click on any individual status icon of a Mako on the right of the list (, or)

The Information Window also contains shortcut links ( ) to change various parameters within the main menu. These parameters are explained in different sections of this manual.

---

i Large sections of the CMS are inoperable if you don't have an appliance selected.

ii In your use of the Mako CMS, you'll find other ways to select a Mako. **Always remember: The Mako you are working with is listed in the Header bar of each page.**



3.5 ADDRESS, SUBNET MASKS, GATEWAYS, DHCP, WINS, DNS, VLAN TRUNK

Configure

An IP Address is simply an identifier for a device or digital service. An addressed device makes requests to other addressed devices for data, and so long as the request is valid, from an authorized requester, for permitted data, the data is sent to the requesting address. This would work perfectly if every Internet device could have a unique address, so no confusion would arise over who was who.

Far from being perfect, the Internet Protocol is actually a large collection of work-arounds to handle a limited number of unique addresses. There is another Internet schema ready-to-go that minimizes this (IPv6), but most people are resistant to change so it's not clear when this new schema will be deployed.

The default settings, pre-configured by your reseller, will usually be fine for your network. But from time to time you may require new features and functionality. Your reseller can advise on the appropriate changes as your requirements change.

Most ISP plans have been pre-configured and the only entry required is selecting the appropriate plan. [i]

Once you've selected a Mako in the Selection menu, you may change its parameters. [ii]

3.5 Address, Subnet Masks, Gateways, DHCP, WINS, DNS, VLAN Trunk

Within the CMS you'll see the above settings being requested several times in different locations. The settings usually have help text associated with them. These definitions are more 'hands-on' than full explanations, aimed at setting up the Mako System quickly, rather than deliver a lesson on the Internet.

IP ADDRESS The address is a four-part dotted-decimal reference used by an Internet device to tell other devices where it is.

An Internet appliance requires at least one address, sometimes more: Your Mako, for instance, is one appliance that houses at least four different, addressable components: LAN 1, LAN 2, Wireless transceiver, Cellular transceiver, router and others.

Local addresses tend to start with **192.168**.x.y, or **10.10**.x.y, or **127.0**.x.y. International addresses do not start with **192**, **127** or **10**.

Your Mako is usually your first device in the Local Area Network (LAN), and often has the address 192.168.1.253 for LAN 1, 192.168.2.253 for LAN 2, etc., but this may change depending on the design of your LAN.

Do not set your IP address to a public Internet IP Address.

Each network should be given a unique address scheme if VPN communications are to be configured.

---

i Be aware that re-configuring these functions can disable critical operations of your Mako appliance — care should be taken to ensure that configuration changes do not compromise your office network security or its access to the Internet.

ii Your ability to configure Makos may be restricted. Please consult your reseller if you encounter any difficulties.

SUBNET MASK

A subnet mask defines what part of the IP Address is used for the network, and what's used for the host.

Each IP Address can be broken down into two areas: the network (part of the IP Address used for routing) and the host (part of the address used as destinations or locations).

A common subnet mask is 255.255.255.0. The binary math won't be explained here, but this subnet mask says the first three parts of the address are used for the network with which to route data, and the last part (numbers 0-255) are reserved for the destinations, or components, in your local network.

NAT

Network Address Translation (NAT) allows LAN addresses to be converted to WAN addresses and back, allowing devices in your LAN to act like they have unique, public IP addresses.

If you've been issued with a public IP network by your ISP and you wish to use this public network on your network port without the Mako performing a NAT function, click Off. With this disabled, PCs connected to this LAN will use real-world IP addressing. Firewall rules still need to be created in order to access these devices. Disabling NAT should only be used with publicly routable IP addresses.

- Changing the NAT status will erase any Firewall rules.

GATEWAY ADDRESS

The IP Address of the modem, router, hub or switch connecting your local network to the Internet via your ISP.

Often this address is automatically configured if using DHCP.

DHCP ON, OFF

Dynamic Host Configuration Protocol (DHCP) allows IP addresses in a network to be assigned automatically to a connected PC when that PC is powered-up. A PC 'leases' an address from a pool of local addresses.

On: This enables the automatic assigning of local IP addresses to connected devices.

Off: New devices will require manual assignment of an IP address in the DHCP Leases page before it can communicate with the network.

When DHCP is Off, **DHCP lease pool**, **WINS** and **DNS server** options will be unavailable.

DHCP RELAY

This disables the DHCP functionality on the Mako and pushes the capabilities to an external DHCP server to handle the DHCP lease assignment for the connected network devices. A VPN connection to the external DHCP server is required. The IP address of one or two remote DHCP servers must be specified in the address fields that are enabled when the relay option is selected.

DHCP ATTRIBUTES

Defines a simple protocol for DHCP internal communication.

Type: TFTP | DOMAIN | NTP Server: Unless otherwise advised, TFTP will suit most networks.

Value: An alphanumeric string, for tagging purposes.

DHCP LEASE POOL

The Mako itself is designated as the DHCP server.

Start: The lowest address for use.

End: The highest address for use.

Defining this pool isn't mandatory and if left blank the Mako will start from the beginning of the IP range. The reason for defining a pool is that you may desire some addresses to be configured by DHCP and have the rest available for static IP allocation.

The IP range will be limited by the defined subnet mask. The range is also dependent on the defined Mako Ethernet IP address: if entered incorrectly or the wrong range is used, this will create an error alert.

WINS SERVER IP (OPTIONAL)

Windows Internet Name Service (WINS) is a Microsoft proprietary function for NetBIOS computer names that maps host names to network addresses.

Enter the WINS address here.

DNS SERVERS

Domain Name Servers (DNS) map numerical-to-alphabetical addresses and back, and these external services are necessary for common Internet operations.

Internet addresses are numerical, but humans prefer alphabetical references for sites and devices. We're more likely to remember www.facebook.com than 69.171.247.29.

You may need to specify the address of internal DNSs, but these are normally set for you, if at all.

Internal DNSs are different from the public DNS addresses specified in the Internet configuration section.

DHCP TTL

Time To Live (TTL) determines how long a device may use an internal address – from one hour to 14 days.

This usually used to set how long a device (such as a laptop on a Wireless connection) may use the LAN before they must re-apply to be on the network.

VLAN TRUNK

The physical LAN that all Virtual LANs (VLANs) will use to send/receive traffic. This checkbox maybe faded out if it has already been selected as a VLAN Trunk, to prevent the accidental deactivation of all VLANs at the physical LAN page (we recommend deactivating VLANs from the **VLAN Setup** page).

You may swap the LAN required by choosing a different LAN for the VLAN Trunk.

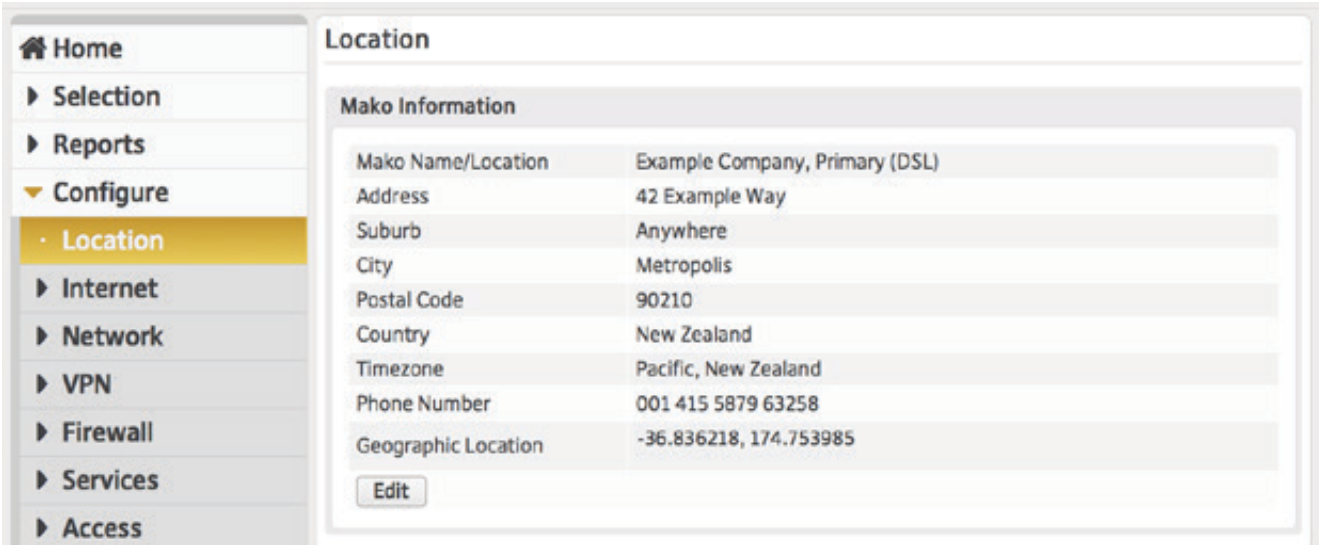
A physical LAN not designated as the VLAN Trunk may operate over the VLAN Trunk by giving that physical LAN a VLAN ID.

Each Mako VLAN requires a VLAN ID – a number from 0-4095. This might indicate that you can run 4096 VLANs over a LAN, but the actual number of VLANs you can effectively run comes down to the amount of traffic your Mako processes at any given time.

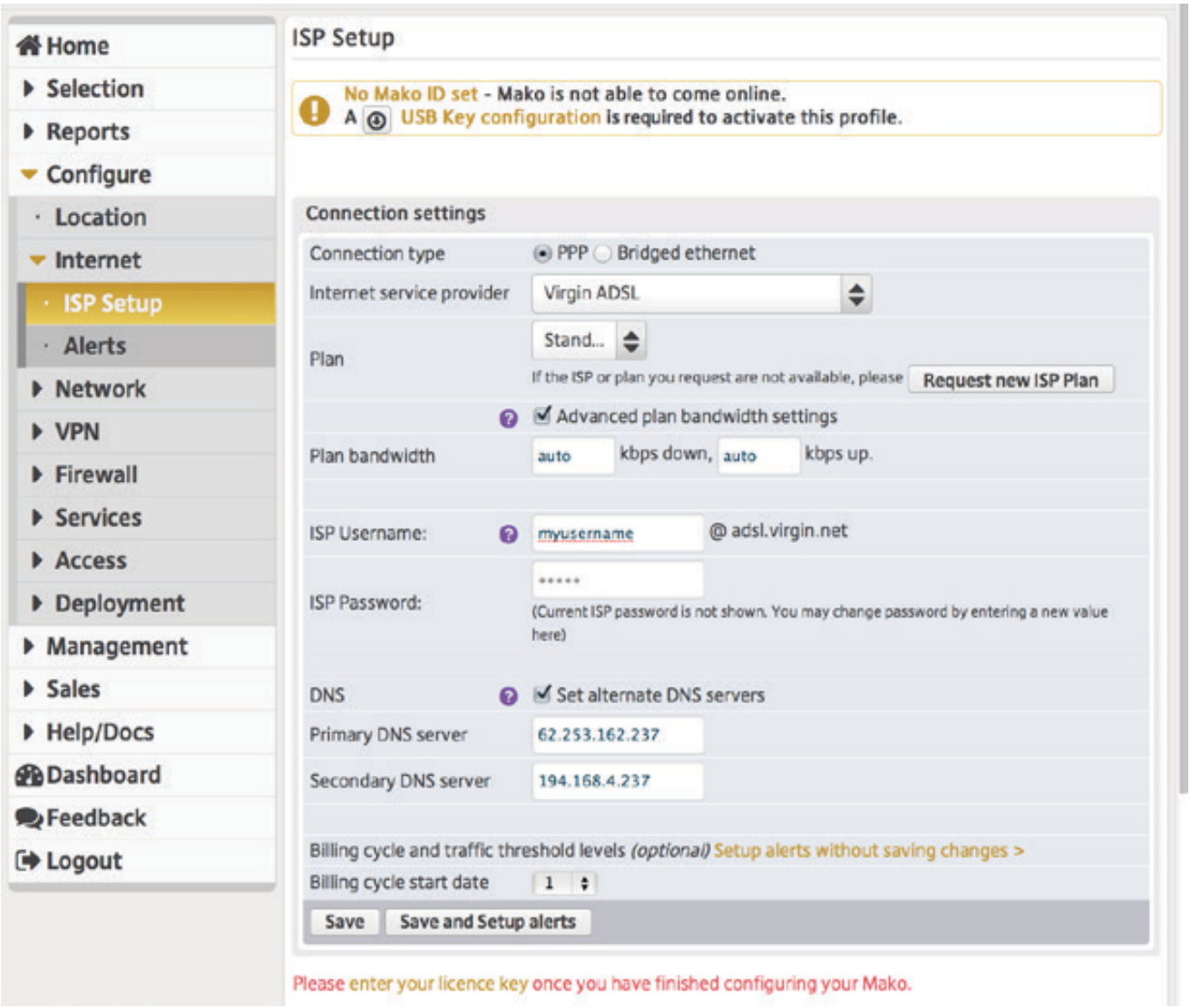
- Only one LAN per Mako appliance may be used to handle VLAN traffic.

VLANS INCLUDED

All configured VLANs and WLANs are listed here.



4 CONFIGURE > LOCATION



5.1 > ISP SETUP

4 Configure › Location

The Location section allows you to update and view the non-technical details of your Mako.

- Click **Edit**. A pop-up window allows you to edit your Mako's details.

Save when finished.

5 Configure › Internet

5.1 › ISP Setup

The Internet Service Provider (ISP) is, most often, a telecommunications company providing your Internet connection.

This section configures your Mako to connect to your ISP. i, ii, iii

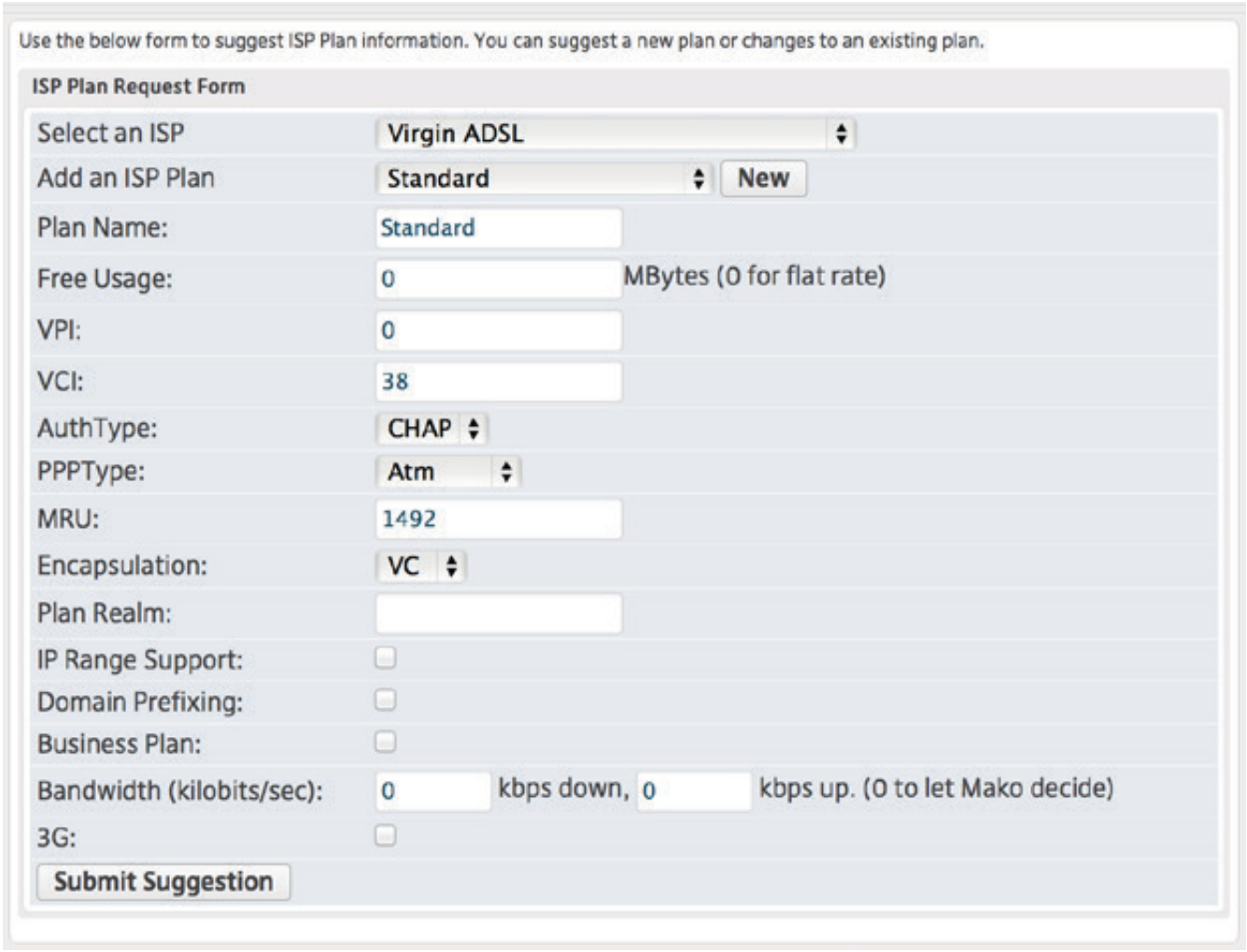
CONNECTION TYPE	Options are dependent on: ■ the Mako model you've selected ■ the connect type–PPP, IP, Bridged Ethernet, DSL, Cellular ■ your ISP plan.
INTERNET SERVICE PROVIDER, PLAN	The CMS provides you with a list of ISPs and common plans. If your ISP and/or plan aren't listed, click the ISP Plan Request to choose the connection type (connection types are limited to the selected Mako).

- Enter the appropriate details in the rest of the page. *Address, Subnet Masks, Gateways, DHCP, WINS, DNS, VLAN Trunk...*
- **Save and Setup Alerts**, or **Save**, when finished.

i Bridged Ethernet should only be used if required by your ISP. It's used when Ethernet frames are to be sent and received directly over the DSL connection.

ii If either IP or Bridged Ethernet are selected, the DHCP, WAN IP, Network Mask and Default Gateways must be configured.

iii IP is only available on Ethernet-connected Makos, and configuration follows 'DHCP Settings'.

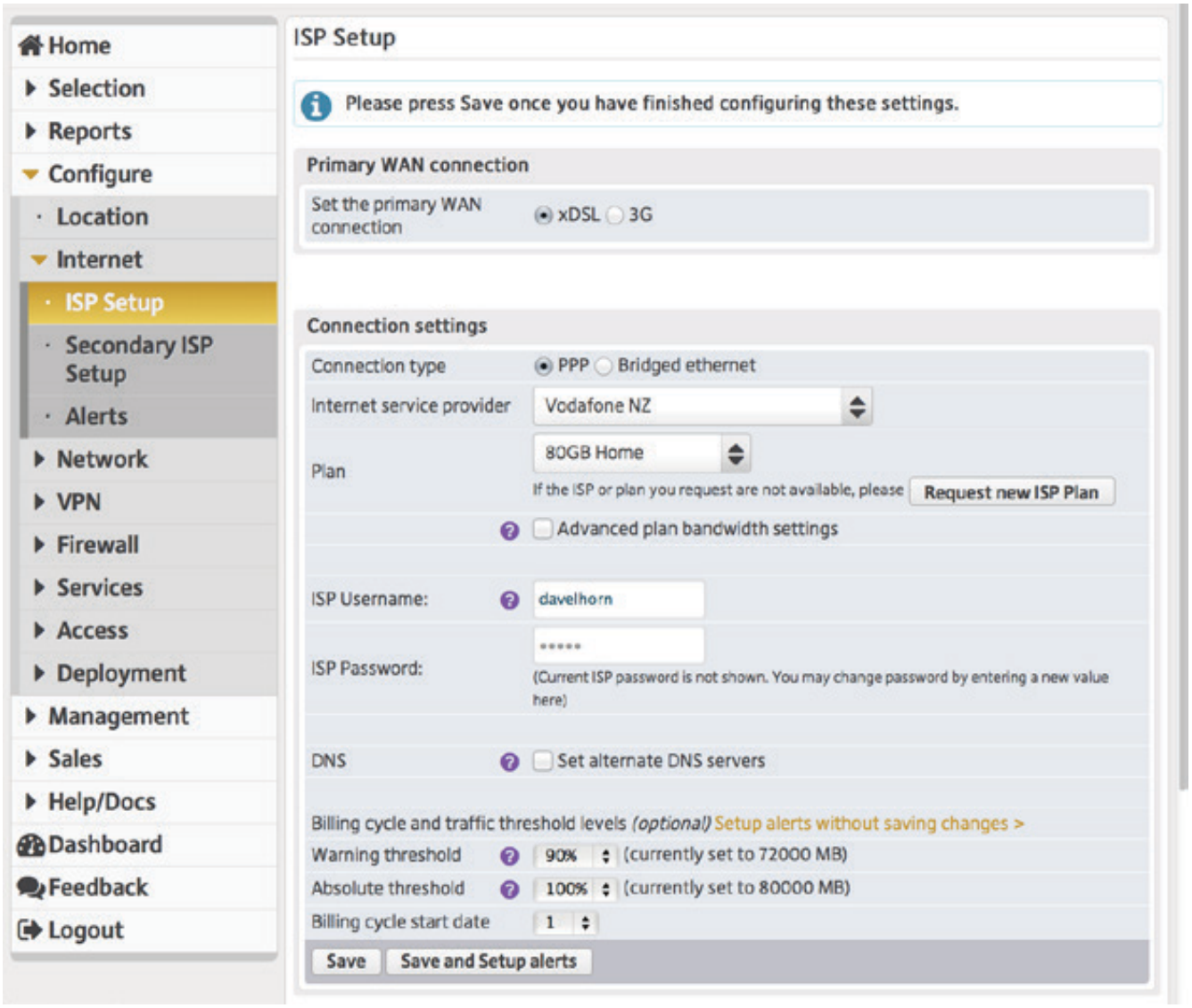


5.1.1 ISP PLAN REQUEST

5.1.1 ISP Plan Request

Plans may be suggested to your Mako System administrators. If you're not sure on some of the settings we suggest leaving the defaults as-is.

SELECT AN ISP	Choose an ISP that you want modified from this list.
ADD AN ISP PLAN	Select a pre-existing plan from the drop down menu to base this new plan on, or click the New button and enter a new plan name in the Plan Name field.
FREE USAGE	Enter the allocated usage in MB, i.e. if it a 10GB plan enter 10 000 here. If it's a flat rate plan, leave this at 0.
VPI	The VPI tells the switches where to route the packet of information, or what path to take. [A VPI of 0 indicates that this is a Virtual Channel Connection (VCC). A non-zero value indicates that this is a Virtual Path Connection (VPC)].
VCI	The Virtual Channel Identifier (VCI), used in conjunction with the VPI, indicates where an Asynchronous Transfer Mode (ATM) cell is to travel over a network.
AUTHTYPE	Choose the authentication type from the drop down menu: Password Authentication Protocol (PAP), 2-way handshake or Challenge Handshake Authentication Protocol (CHAP), 3-way handshake.
PPTP TYPE	Choose the type of Point-to-Point Tunneling Protocol (PPPT) used for this plan from the drop down menu, Asynchronous Transfer Mode (ATM) or Ethernet.
MRU	The Maximum Receive Unit (MRU) is the size of the largest packet the Mako will accept. Increasing the MRU means larger incoming packets, which in turn increases transmission errors as the whole packet must be retransmitted. The recommended minimum is 250 and maximum is 1500.
ENCAPSULATION	Choose the encapsulation type from the drop down menu, Virtual Concatenation (VC) or Logic Link Control (LLC).
PLAN REALM	Enter the URL of the ISP here.
IP RANGE SUPPORT	Your ISP may have provided you with a range of IPs your Mako may handle. Checking this box allows access to the 'IP Range' page in the CMS (subject to the plan's approval).
DOMAIN PREFIXING	Check this box if you use domain prefixing. Domain Prefixing allows users to create subdomain labels, usually for service-routing. For example, a company called Fubar may have a public web domain at **www.**fubar.net, but want a members-only service at **members**.fubar.net. Here, 'members' is a registered domain prefix.
BUSINESS PLAN	This checkbox indicates if the suggested plan is a cellular plan. Check this box if true.



5.2 PPP ACCOUNT SETTINGS

5.2 PPP Account Settings

Point-to-Point Protocol (PPP) is mainly used for an DSL configuration to establish a direct connection between two networking nodes. Your ISP should have sent you the initial username/password details.

ISP USERNAME, ISP PASSWORD	Enter the relevant ISP details here.

5.3 Cellular Settings

The following options apply if you are using a cellular network for connectivity, or your Mako allows for a cellular failover solution. i

CAUTION: We recommend NOT having a cellular connection as your Primary for two reasons. First, it's costly to run. Second, the Mako System is geared to use cellular connections as a backup feature called Cellular Failover, and only one SIM card may be used per device at any one time. Cellular Primary connections are offered to support rural or isolated areas with no DSL or Ethernet infrastructure.

For more about Cellular Failover, see the **Secondary ISP Setup** section.

SIM CARD PIN, SIM CARD PIN AGAIN	Enter your PIN twice. Please enter the PIN manually rather than copy/paste.
ACCESS POINT NAME (APN)	Enter your APN (your ISP plan selection may have filled this in for you). It tells your carrier what type of network gateway your system should use.

5.4 Bridged Ethernet Settings

Bridged Ethernet connections are special arrangements between you and your ISP, or within large networks, which allow one network to act as an 'internal extension' of another. They're generally not required unless by special mandate.

SET ALTERNATE DHCP SERVER	Check the box to manually configure an alternate DHCP service.
MAKO WAN IP	The external address allocated to the Mako
NETWORK MASK	Often set to 255.255.255.255 to allow allocation across all IP ranges.
DEFAULT GATEWAY	The address of the router handling DHCP.

i If 'Cellular' is chosen as the primary connection, Cellular failover is not available.

5.5 Billing Settings

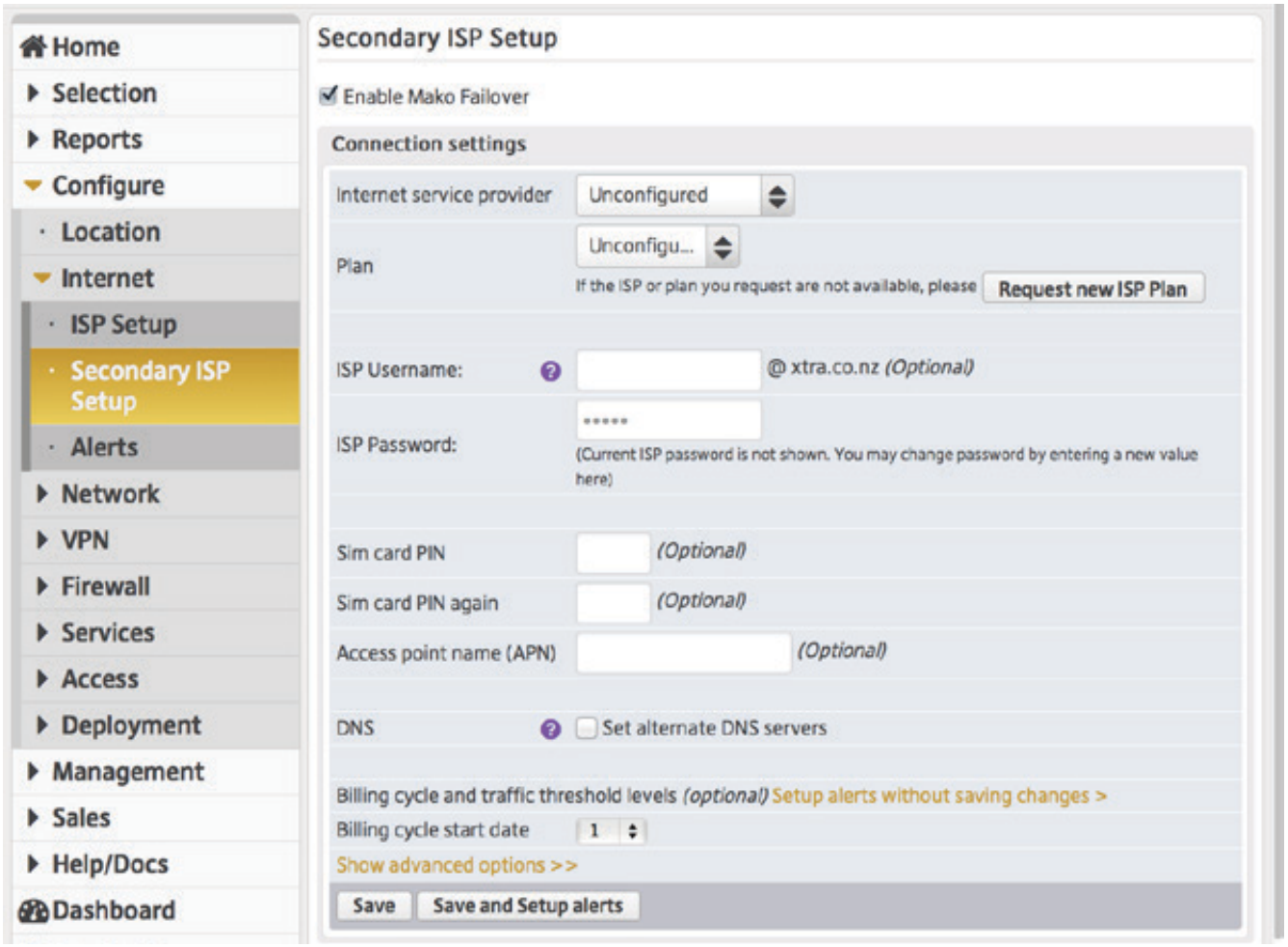
The following options concern your billing cycle and monthly traffic thresholds. i

BILLING CYCLE START DATE	Day of the month your ISP's bills are due. This date is important for correctly calculating data usage over time.
WARNING THRESHOLD	A percentage of your bandwidth allowance for the month – useful when on a limited bandwidth ISP plan.
ABSOLUTE THRESHOLD	A percentage of your bandwidth allowance for the month. (This is often higher than the plan arranged with your ISP to handle high traffic.) An Absolute Threshold is necessary if your ISP has imposed traffic limits on your account. If this is selected, and the threshold is reached your Internet connection will be cut off when this threshold is reached. It can be reactivated with manual intervention but your connection will remain disabled until then.

5.6 Considerations

- If you wish to change your ISP Password you must be sure to also change it with your ISP. Take special care to ensure that the password is entered exactly the same at both places (your reseller and your ISP).
- Don't forget to click **Save** to save your changes before leaving this page.
- Select a plan similar to the one you have, or if your plan doesn't match the ISP offerings, click on the **ISP Plan Request** link next to the Internet Service Provider drop menu. This form provides various configuration options for this plan. It isn't necessary to provide all the details, as this is a suggestion request, not an actual configuration. It's better to provide as many known details as possible to ensure that the requested plan meets the requirements of your ISP offering.

i This facility is not available where your ISP Connection Plan does not impose a traffic-charging threshold. Threshold alerts are not visible until an ISP Plan has been selected for your Mako.



5.7 > SECONDARY ISP SETUP > CELLULAR FAILOVER

5.7 > Secondary ISP Setup > Cellular Failover

This page is accessible if your Mako is LTE or 3G-capable, and a cellular connection is not your Primary Internet connection.

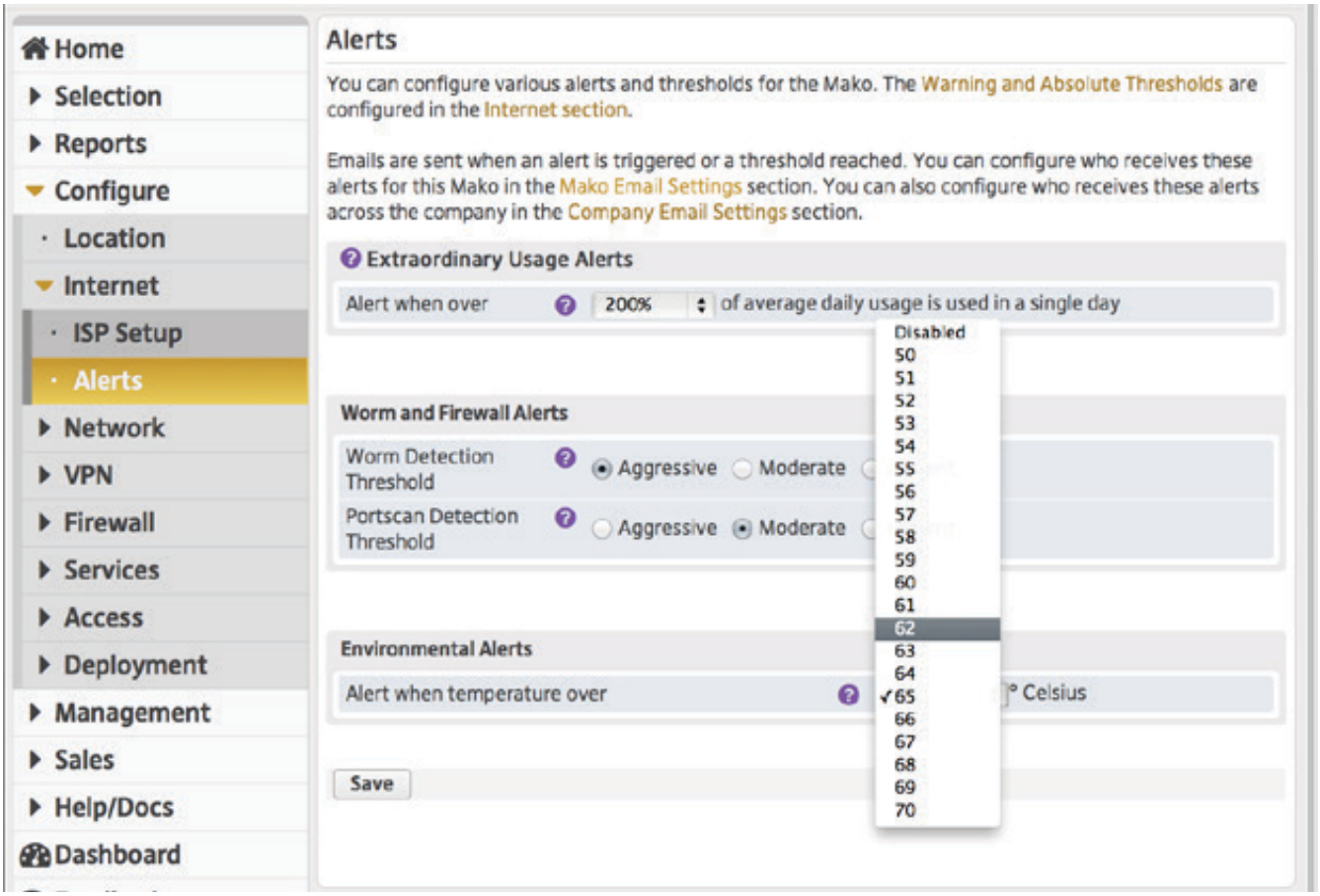
If your main network connection (PPTP, Ethernet, etc) is interrupted, cellular-capable Mako systems are able to switch to a cellular network for continued operation. If cellular failover is required, ensure that the Mako has an active SIM card inserted into the slot and is within your provider's coverage area. i

- Check the **Enable Cellular Failover** box.

INTERNET SERVICE PROVIDER	Your cellular carrier (this might not be the same as your primary provider).
PLAN	Your cellular plan type.
SIM CARD PIN/ SIM CARD PIN AGAIN	Enter the SIM card details. This is optional, since not all SIM cards are secured this way. Re-type your SIM PIN manually, as an incorrect copy/paste will not reveal if you've made a mistake in entering it the first time. Note: These fields are not a facility for assigning a PIN to your SIM; this can be configured on most mobile phones.
ACCESS POINT NAME (APN)	This should already be populated from the ISP selection. This can be changed if instructed by your cellular provider.

- **Save**, or **Save and Setup Alerts**, when finished.

i We recommend testing this failover ability occasionally outside of your business hours.


Home
Selection
Reports
Configure
Location
Internet
ISP Setup
Alerts
Network
VPN
Firewall
Services
Access
Deployment
Management
Sales
Help/Docs
Dashboard
Alerts
You can configure various alerts and thresholds for the Mako. The Warning and Absolute Thresholds are configured in the Internet section.
Emails are sent when an alert is triggered or a threshold reached. You can configure who receives these alerts for this Mako in the Mako Email Settings section. You can also configure who receives these alerts across the company in the Company Email Settings section.
Extraordinary Usage Alerts
Alert when over
200%
of average daily usage is used in a single day
Disabled
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
Worm and Firewall Alerts
Worm Detection Threshold
Aggressive
Moderate
Portscan Detection Threshold
Aggressive
Moderate
Environmental Alerts
Alert when temperature over
° Celsius
Save

5.8 > ALERTS

5.8 › Alerts

5.8.1 Extraordinary Usage

Over time, the Mako System builds a profile for the usual traffic patterns of your Internet connection. Extraordinary usage is outside the norm for your Mako's internet connection. You can set threshold alerts to trigger when the volume of extraordinary traffic is attained.

5.8.2 Worm Alerts

Your Mako automatically detects PCs on your network that are infected with worms (self-replicating malware computer programs) and stops the infected PCs from accessing the Internet. Choose your level of detection sensitivity.

5.8.3 Firewall alerts

Your Mako detects unapproved probes scanning your network for vulnerable or open IP ports. Choose your level of detection sensitivity.

5.8.4 Environmental Alerts

Your Mako monitors its temperature, which can be affected by an external heating or cooling source.

ALERT WHEN OVER (%)	A percentage of your bandwidth allowance for the day. Useful when on a limited bandwidth ISP plan. This threshold alert helps manage your DAILY traffic, while the ISP Setup page will contain MONTHLY threshold warnings. If a secondary WAN (normally cellular) has been enabled a second Extraordinarily Usage Alert may be configured.
WORM DETECTION THRESHOLD	Aggressive | Moderate | Lenient. Threshold levels relate to the number of connections detected per 10-minute period. The scores for Aggressive, Moderate and Lenient are 1000, 1800 and 3000 connections respectively. More intense threshold levels may impact on your Mako's connection speeds.
PORTSCAN DETECTION THRESHOLD	Aggressive | Moderate | Lenient
ALERT WHEN TEMPERATURE OVER	Set your upper level operating temperature.
FAN SPEED ALERT	High-capacity models contain an internal fan. Check if internal cooling fans require monitoring.

- **Save** when finished.

5.9 › IP Range

This page is available if the ISP Plan allows your Mako to allocate ranges of IPs over your Mako. It allows you to review your Public IP address settings if your ISP provides you with more than one. The information on this window will be set by your reseller and in most cases will not require modification. i

EXISTING IP RANGES This table lists the current IP ranges for this Mako.

5.9.1 Add IP Range

PUBLIC IP ADDRESS Enter a new range here, or click [Single IP Mask] for a single address.

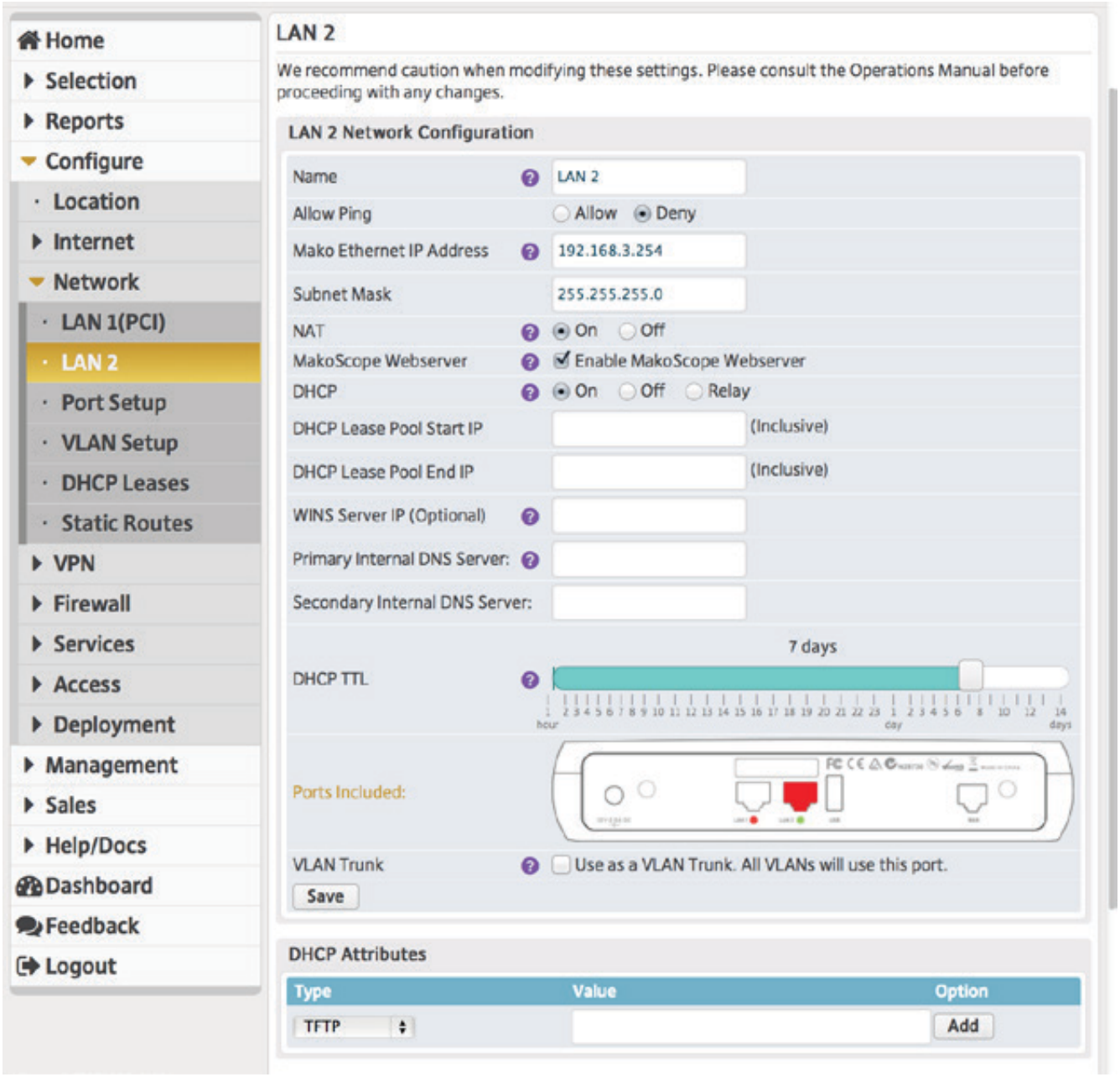
- **Add** when finished.

5.9.2 Public IP Address

PUBLIC IP ADDRESS Defines the address to use when performing NAT operations from LAN to WAN. Only change this setting if you have a publicly routable range terminating on the Mako's external address.

- **Use Default** when finished.

i If your ISP doesn't provide you with multiple IP addresses, this page won't be available. *ISP Plan Request...*


Home
Selection
Reports
Configure
Location
Internet
Network
LAN 1(PCI)
LAN 2
Port Setup
VLAN Setup
DHCP Leases
Static Routes
VPN
Firewall
Services
Access
Deployment
Management
Sales
Help/Docs
Dashboard
Feedback
Logout
LAN 2
We recommend caution when modifying these settings. Please consult the Operations Manual before proceeding with any changes.
LAN 2 Network Configuration
Name
LAN 2
Allow Ping
Allow
Deny
Mako Ethernet IP Address
192.168.3.254
Subnet Mask
255.255.255.0
NAT
On
Off
MakoScope Webserver
Enable MakoScope Webserver
DHCP
On
Off
Relay
DHCP Lease Pool Start IP
(Inclusive)
DHCP Lease Pool End IP
(Inclusive)
WINS Server IP (Optional)
Primary Internal DNS Server:
Secondary Internal DNS Server:
7 days
DHCP TTL
hour
day
days
Ports Included:
VLAN Trunk
Use as a VLAN Trunk. All VLANs will use this port.
Save
DHCP Attributes
Type
Value
Option
TFTP
Add

6.1 > LAN [N]

6 Configure > Network

6.1 > LAN [n]

Each Mako will have 2 or more physical LANs to configure, so there will be the requisite number of LAN pages available.

Your network is pre-configured by your reseller, therefore changes shouldn't be necessary. We recommend keeping a record of the existing settings so you can go back to them if the new settings don't work.

6.1.1 LAN Network Configuration

You're able to rename each LAN on your system and this name will be reflected in the left menu navigation of the CMS. We suggest you choose a name more meaningful to you (eg. LAN 2 --> 'Public') if necessary.

We have a number of Help tips (?) throughout the CMS to assist you through this section. i

NAME	Rename your network to something more meaningful to you (such as Secure Network, Office Network, DMZ, etc.)
ALLOW PING	'Allow' lets the Mako respond to 'ping' traffic on the LAN. Ping is used to test the 'reachability' of a host using Internet Control Message Protocol (ICMP). The default is **Deny** and should only be enabled when troubleshooting.

For common settings: *Address, Subnet Masks, Gateways, DHCP, WINS, DNS, VLAN Trunk...*

6.1.2 Configuration-Dependent Options

Depending on the Mako being configured and your reseller or administrator's settings, other options will be available to you on this page.

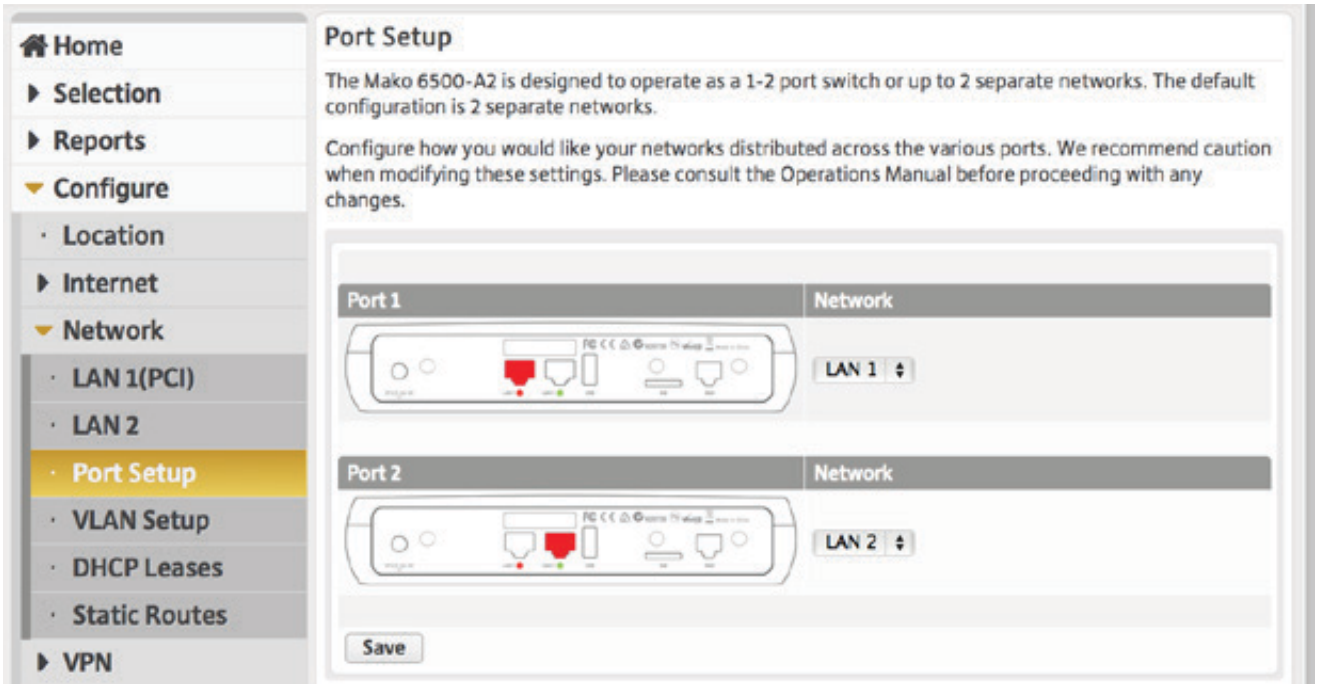
PORTS INCLUDED	Displays an illustration of the rear ports of the selected Mako and highlights the selected port in red. Click Ports Included to configure the LAN's available ports.
VLAN TRUNK, VLANS INCLUDED, VLAN ID	A VLAN Trunk is a port that handles traffic for all configured VLANs. VLAN Traffic going across the Trunk is tagged with the 802.1Q VLAN ID in the Ethernet frame. If one or more VLANs already exist, they will be **link-listed** under **VLANs Included**. Links will take you to the *> VLAN Setup...* page, should you need to re-configure them.

- **Save** when finished.
- Enter the appropriate details in the rest of the page. *Address, Subnet Masks, Gateways, DHCP, WINS, DNS, VLAN Trunk...*

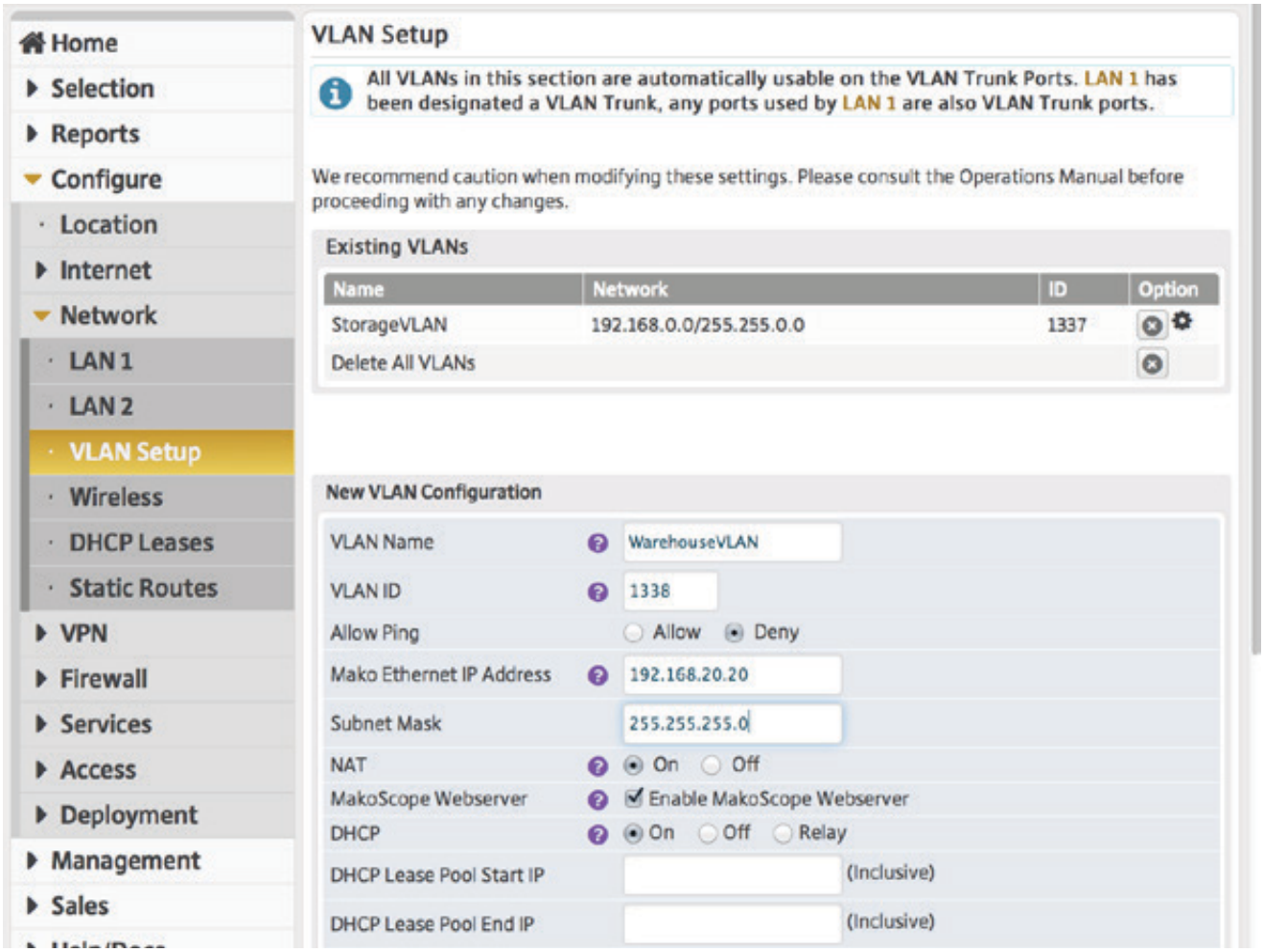
6.1.3 Other considerations

Please take careful note of all caution messages. These messages will vary depending on the situation. You need to be aware of these messages and amend the situation if possible.

i When making changes to any of these configuration options, click **Save** to update the details. There are no save prompts when leaving this page and all unsaved changes will be lost.



6.2 > PORT SETUP



6.3 > VLAN SETUP

6.2 › Port Setup

Here you configure how you would like your networks distributed across the various ports. You can also merge the separated ports to operate as a bridged network, creating one logical LAN with 2 ports.

The illustrations may differ from Mako to Mako, depending on model. **i**, **ii**

6.3 › VLAN Setup

VLANs are virtual LANs, a way of simulating distinct data paths while using the same physical LAN by tagging data packets with VLAN IDs. For common settings: *Address, Subnet Masks, Gateways, DHCP, WINS, DNS, VLAN Trunk...*

VLANs will not be usable until a VLAN trunk has been enabled. Navigate to the LAN that is to be configured as a VLAN trunk and check the VLAN option.

6.3.1 Existing VLANs

NAME	Name of the VLAN. If any VLANs exist, there's a **Delete All VLANs** entry here.
NETWORK	IP Address/Mask of the VLAN address space.
ID	The numerical ID of the VLAN tagged to data packets. As VLANs share a physical LAN, this ID ensures mixed data packets go to the right devices.
OPTION	This section lists the VLANs in scope for your system. : Deletes the VLAN. : Edit options for this VLAN. A new window appears

6.3.2 New VLAN Configuration

Setting up a VLAN is nearly identical to setting up a physical LAN. *Address, Subnet Masks, Gateways, DHCP, WINS, DNS, VLAN Trunk...* with the addition of a VLAN ID.

The VLAN ID is a number from 0 to 4095 **iii**. The VLAN ID is unique across all VLANs: no VLANs may share the same VLAN ID, even if each VLAN is configured for different subnets. **iv**

VLAN ID	Enter a unique ID for the new VLAN.
TRUNK PORTS	If a VLAN Trunk is configured, enter your port info here.

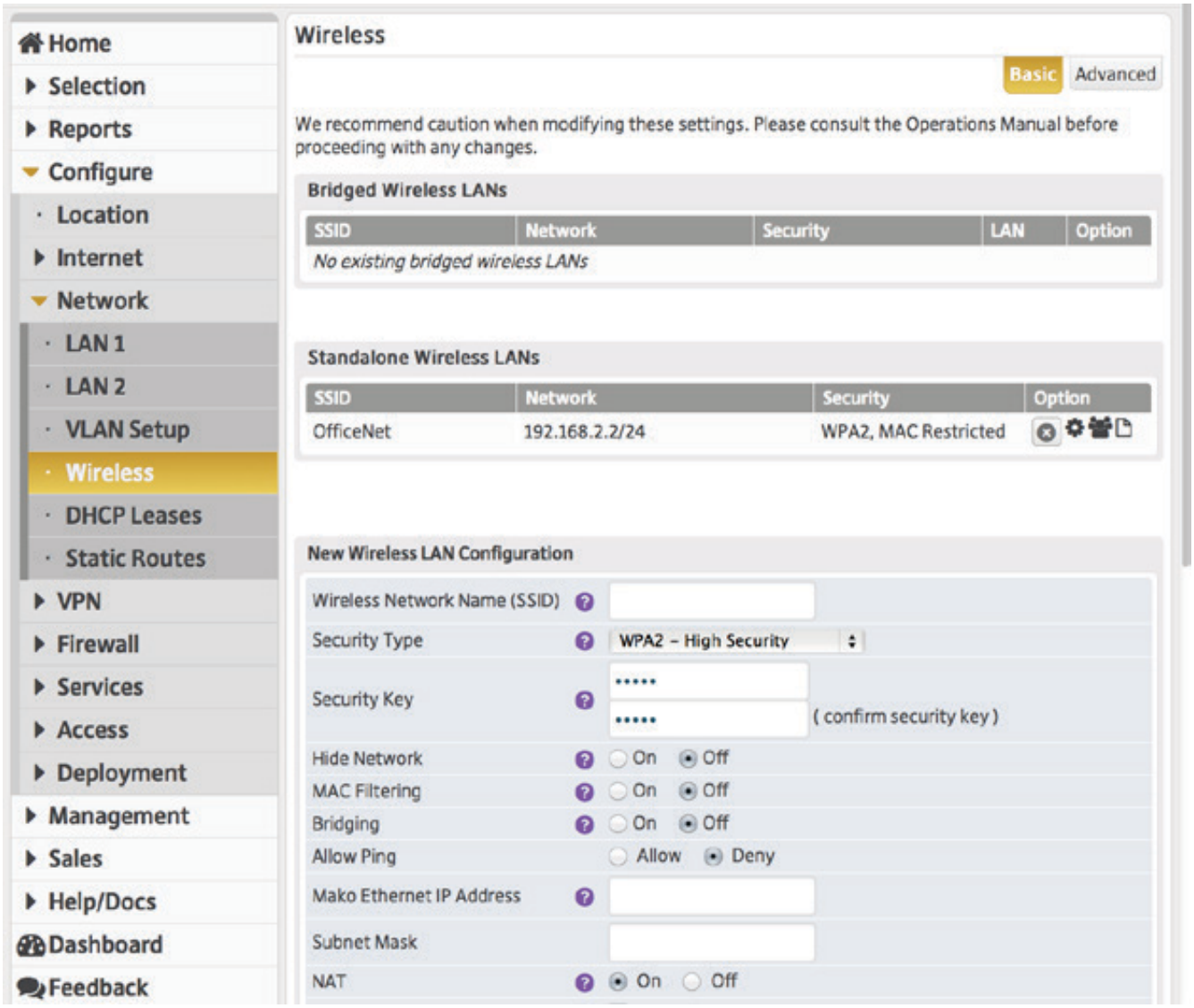
- Add New VLAN when finished.

i The Port Setup page is only visible if your Mako model has more than 1 port available for configuration.

ii Merging, separating or rearranging LAN ports will remove the settings for each LAN included in the change.

iii For ease of reference, many use the IP address of the VLAN as the ID, so if the VLAN's IP Address is 192.168.1.123, then the VLAN ID is "123".

iv This means the theoretical maximum number of VLANs a Mako device can handle is 4096, though in practice, few Makos use more than about 20,



6.4 > WIRELESS LAN > BASIC

6.4 > Wireless LAN > Basic

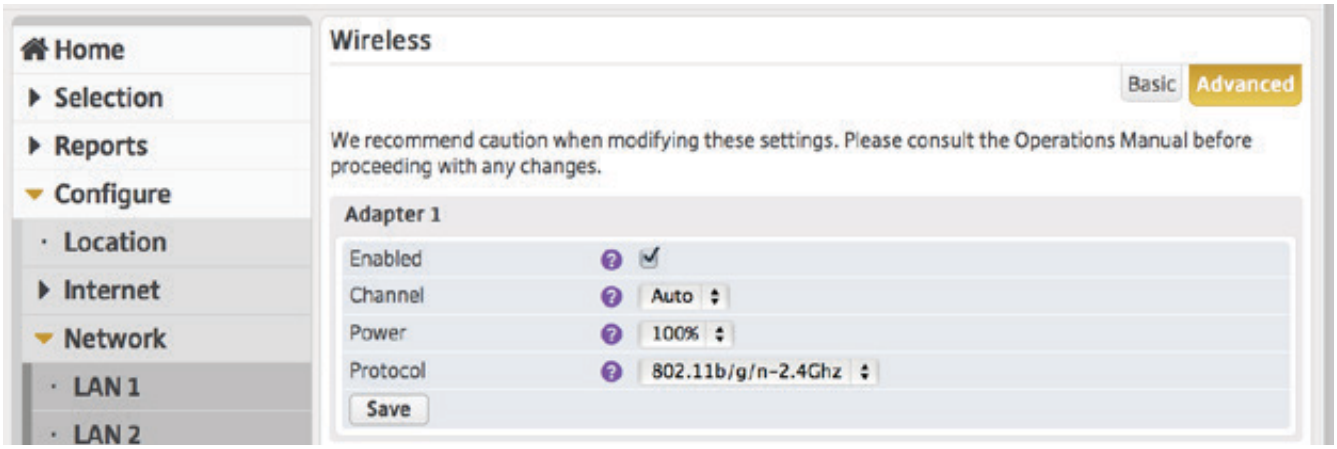
Setting up a Wireless LAN (WLAN) is similar to setting up a physical LAN. Some options may or may not be available to your Mako depending on make, permissions or pre-configured function.

WIRELESS NETWORK NAME (SSID)	The name of the Wireless LAN. Users will see this name when selecting what network to join, so be cautious about including company-sensitive labels, like names, locations, operating systems etc.
SECURITY TYPE	**Open** security has no password, and anyone can join the network. **WPA2** is high security for all networks dealing with sensitive information.
SECURITY KEY	**(WPA2 Only)** Specifies the password to protect the Wireless LAN.
HIDE NETWORK	Specifies if users are able to see this Wireless LAN when searching for networks, or if they have to know the name of the network before they can join. Hidden networks offer additional security and are recommended for internal Wireless networks. Hidden networks aren't recommended for public networks like cafés or libraries.
MAC FILTERING	MAC filtering specifies if only approved devices with a hard-coded MAC address (most computing/communications devices) can connect to the Wireless LAN.
BRIDGING	Extends the LAN over a Wireless network.
ALLOW PING	Allow/Deny people to check if the Wireless LAN is operating.
MAKO ETHERNET IP ADDRESS	The dotted-decimal address of your Mako on the network.

- **Add Wireless LAN** when finished.

Bridged Wireless LANs: Other LANs with which your Mako may share data. Standard options exist for reference, deletion and re-configuration, if permitted.

Standalone Wireless LANs: Wireless LANs your Mako might use, access permitting, with similar reference data.



6.5 > WIRELESS LAN > ADVANCED

6.5 > Wireless LAN > Advanced

ENABLED To use Wireless LAN, this should be checked. When disabled, all Wireless networks will be unavailable and the Wireless LAN unconfigurable.

CHANNEL A channel is a sub-band of the Wireless LAN signal range. Setting the channel number appropriately provides one way to avoid sources of Wireless interference.

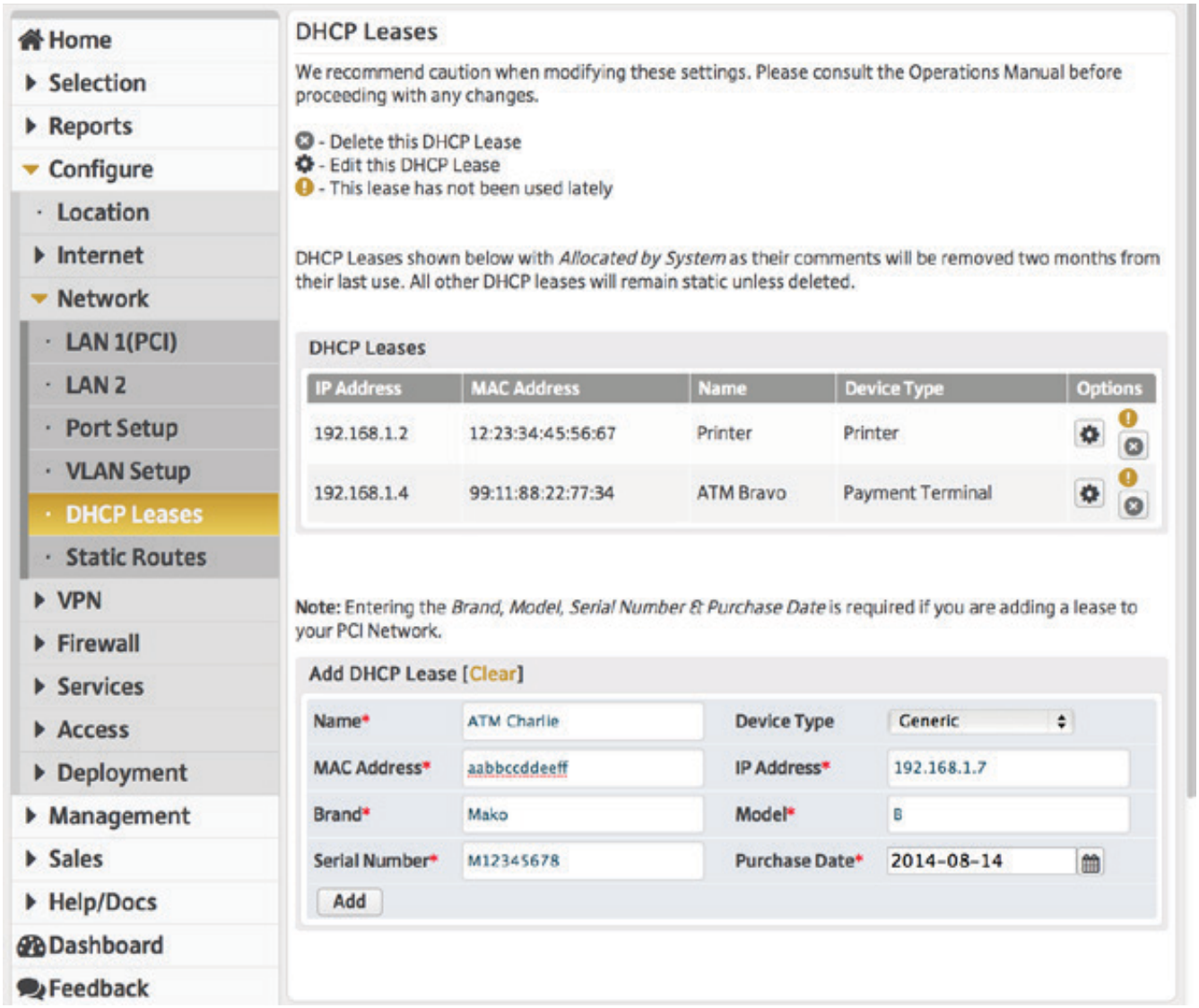
Auto: The best channel will be selected (recommended). For optimal performance, the channel should be 3 channels away from other Wireless networks in the area. For 2.4 GHz networks, this means channels 1, 6 and 11 typically offer the least interference.

POWER Determines the signal strength, and thus the range of the Wireless network. When using secure networks, you may wish to reduce the power output to limit the range of the Wireless LAN.

PROTOCOL Specify the type of 802.11 protocol to use; **b/g/n** or just **b/g**.

802.11 protocol	Release Year	Freq (GHz)	Bandwidth (MHz)	Indoor Range (m)
b	1999	2.4	20	~35
g	2003	2.4	20	~38
n	2011	2.4/ 5	20/40	~70

Once connected, the configured Wireless LAN will be listed in the connected Wireless LAN tables.



6.6 > DHCP LEASES

6.6 › DHCP Leases

A DHCP Lease in your local network is an address reserved for a specific device. It may be inside or outside your DHCP Lease Pool, as defined in the Configure > Network > LAN pages.

Address, Subnet Masks, Gateways, DHCP, WINS, DNS, VLAN Trunk...

6.6.1 Adding a DHCP Lease (Manual Method)

- Enter all the details in the lower table.
- **Add** when finished.

On refresh, the entry will appear in the table above as a static IP address. [i]

6.6.2 Adding a DHCP Lease (Auto-Detect Method)

- Plug the Mako into the network port and power it up.

The Mako system will automatically identify this device and allocate the next available IP address to it. In the **Name** column it will be referred to as "Allocated by system." [ii]

- Click the ⚙. Configure the necessary settings.
- **Save** when finished.

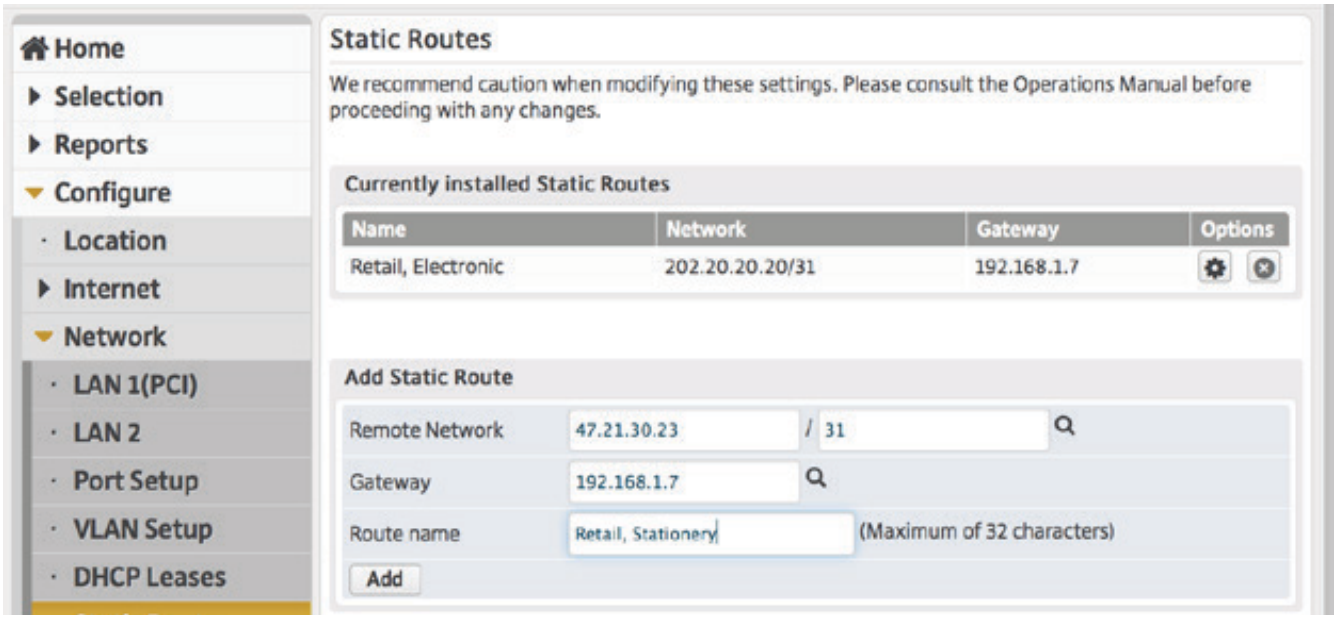
6.6.3 Edit/Delete a DHCP lease

- Click the appropriate icon, ⚙ or ⊘, to change or delete the lease.
- Save when finished.

---

[i] The Mako Add DHCP Lease table will only have the Brand, Model, Serial Number and Purchase Date fields if PCI networks have not been defined for the LAN port.

[ii] It's a good idea to give your device a name you can readily understand and identify. In the Reports section traffic breakdowns are listed by device, and if the device doesn't have a defined name MAC IDs are used instead.



6.7 > STATIC ROUTES

6.7 › Static Routes

You may enter routes to other networks that have routers on one of your LANs. Devices attempting to reach this network through the Mako will be sent an ICMP redirect message which advertises the correct gateway to use. Devices dishonoring or ignoring ICMP redirects may require static routes for access.

Normally this is configured by your reseller and changes shouldn't be necessary.

CURRENTLY INSTALLED STATIC ROUTES	Lists all currently installed static routes. The routes can be deleted or edited.

6.7.1 Add Static Route

REMOTE NETWORK	Enter the IP address and subnet mask here. You can open the Network Helper window by clicking 🔍.
GATEWAY	Enter the appropriate gateway address here. Click on the DHCP Lookup 🔍 to list devices by their DHCP leases, on your network.
ROUTE NAME	Enter a user-defined name for this route (max. 32 characters).

- **Add** when finished.

7 Configure > VPN

A Virtual Private Network is a secure peer-to-peer network that allows private data transmission between Makos and/or third party devices. VPN Networks are composed of direct, secure connections to other devices called **tunnels**. Mako appliances have three types of VPN tunnels available: **Mako to Mako**, **Remote Access** and **Third Party Device**.

7.1 IPSec vs. PPTP: Overview

The Mako System permits two types of Remote VPN connection: **IPSec** and **PPTP**.

IPSec is more complicated to set up and generally requires additional software on the client but is very secure. IPSec uses a Pre-Shared Key as well as your username and password to connect, and may require some third party software depending on your operating system.

PPTP uses a username/password combination and should work with native software in your operating system. PPTP is less secure but easier to setup.

Both VPN types are encrypted.

For security reasons, the PPTP option is disabled for:

i Makos that have licensed the PCI DSS add-on, and;

ii user accounts able to view Mako Reports.

These users must create a separate PPTP VPN username and password. [i]

Any user recorded in the following **Add User** section can have their network access enabled and disabled as appropriate. We recommend that users are permitted access only while they need to use the office network. At other times, their access should be disabled.

7.2 Left Peer/Right Peer Convention

IPSec is a peer-to-peer network protocol where each device in a tunnel has their own incoming and outgoing packet rules. In the Mako System the term **'Left Peer' is used to determine from which device the VPN tunnel was created**. [ii]

Example: If you're creating a VPN tunnel in the CMS between two Makos called 'Alpha' and 'Beta', and you have 'Beta' selected as your Mako in the CMS, the VPN will be created from 'Beta's end. Therefore, Beta is the **Left Peer**.

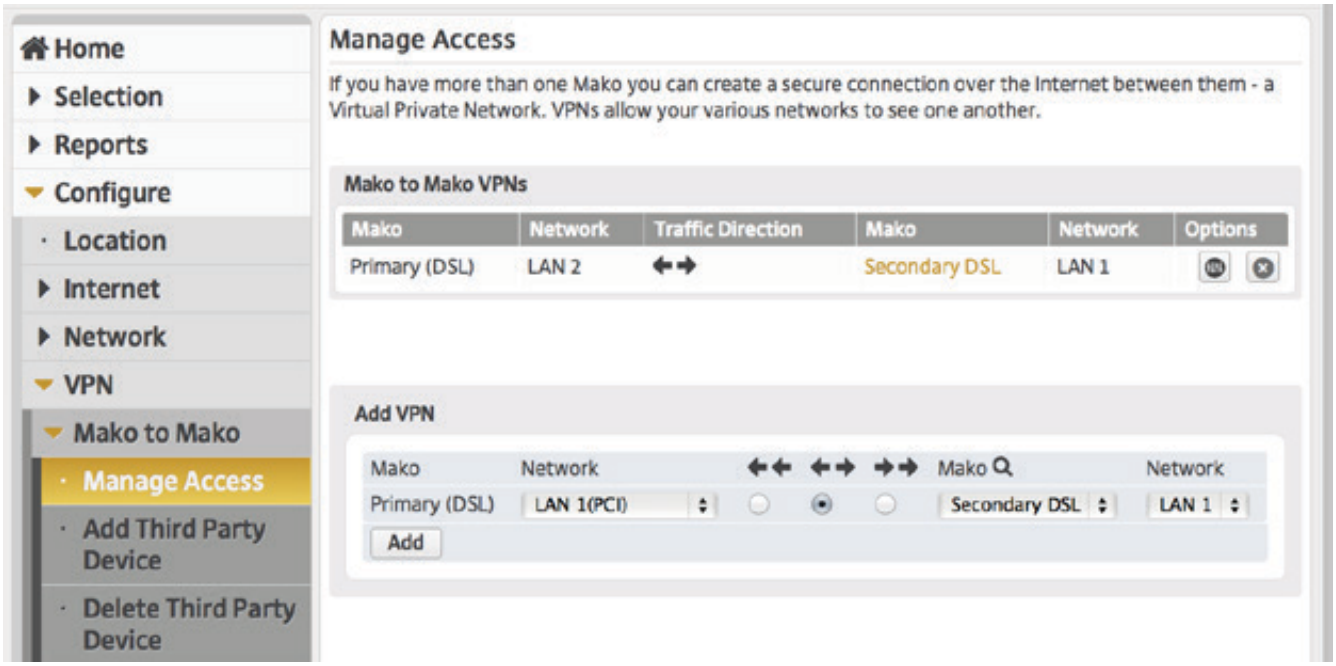
Throughout the VPN section, the Mako from which the VPN was created will be listed on the left-most column of all forms and tables. Mako selection links are also automatically generated in the tables/forms, so you may instantly select the other Mako in the connection to review its VPN rules.

The distinction between left and right peer endpoints in a VPN tunnel has little use for people, but is important for the devices themselves.

---

[i] For security reasons, you must create VPN-Only username and password combinations in the Add Users section in order to access Remote VPNs. Usernames and Passwords that are already used to access your reseller's website cannot access Remote VPNs.

[ii] "Source/destination", "client/server", "master/slave" etc are misleading terms for IPSec tunnels: each device is equal in the eyes of IPSec, and just because one device in a tunnel is told to send data to another, that other device also has its 'right' to reject it. But even in peer-to-peer networks we need a way to distinguish them.



7.3 > MAKO TO MAKO > MANAGE ACCESS

7.3 > Mako to Mako > Manage Access

Use this page to set up VPNs between each pair of Mako-protected networks. The Makos have to be online and operating and each configured with a unique WAN address.

7.3.1 Mako to Mako VPNs

This form lists the current list of VPNs for the Home Mako.

MAKO	Name of the Left Peer Mako at which the VPN tunnel was created.
NETWORK	Name of the Left Peer LAN over which this VPN operates.
TRAFFIC DIRECTION	The permitted direction(s) traffic may be passed between these Makos.
MAKO	The name of the Right Peer Mako.
NETWORK	Name of the Right Peer LAN over which this VPN operates.
OPTIONS	: Advanced settings for VPN properties. : Delete this VPN.

7.3.2 Add VPN

This form allows you to create a VPN between the selected Mako and another.

- Choose the selected Mako's LAN to use for this VPN.
- Choose access rights over the VPN link with the radio buttons.

MAKO	The selected (Left Peer) Mako.
NETWORK	The selected Mako's LAN to use for this VPN.
DATA DIRECTION	← ← The Destination PCs can see those connected to your Home Mako, but not the reverse. ← → Your Home Mako PCs can see the Destination PCs and vice versa. → → The Home PCs can see those connected to your Destination Mako, but not the reverse.
MAKO 🔍	Name of the Mako to connect to. Clicking the 🔍 icon will allow you to search for Makos to connect with the selected Mako.
NETWORK	The LAN name of the Destination (Right Peer) Mako for this VPN.

- **Add** when finished.

7.3.3 Considerations

As a default, each Mako has their own local private network IP address. For example, the Auckland, LAN 1 may use the address range: **192.168.1**.xxx, while Head Office LAN 1 would be **192.168.3**.xxx (where xxx is the range of addresses used at each network).

The significant element is the highlighted '**192.168.1.**' and '**192.168.3.**' — these must be different at the two ends of the VPN link. Please contact your reseller if you have any questions regarding the best choice of private IP addressing schemas for your offices.

The corresponding changes to the secure profile of the Mako at the other end of the VPN link will be made automatically. It isn't necessary to update both configurations. This makes it straightforward to set up or remove a secure link between your Mako appliances.

7.4 > MAKO TO MAKO > ADD THIRD PARTY DEVICE

7.4 > Mako to Mako > Add Third Party Device

Use this page to create a Third Party Device capable of establishing a VPN with your Mako.

If you use a non-Mako router to connect to the Internet at a remote site, you can create a VPN connection between your Mako and the third-party device. Both the Mako and the third-party device should have static public IP addresses in order that the VPN be kept alive for any length of time. i

The third-party device must support:

- IPSec ESP VPNs.
- 3DES or AES-128 encryption algorithm.
- MD5 or SHA1 message digest algorithm.
- Diffie-Hillman 1024 Public Key algorithm.
- Support for Pre-Shared Key Authentication.

7.4.1 Third Party Device

LOCATION	A description of the device. It could be a description of some kind, a name or some other identifying label.
PUBLIC IP ADDRESS	The device's dotted-decimal address as given by its ISP.
NETWORK ADDRESS	The device's local dotted-decimal address and mask in CIDR notation.

- **Add**, or **Add and Create VPN** when finished.

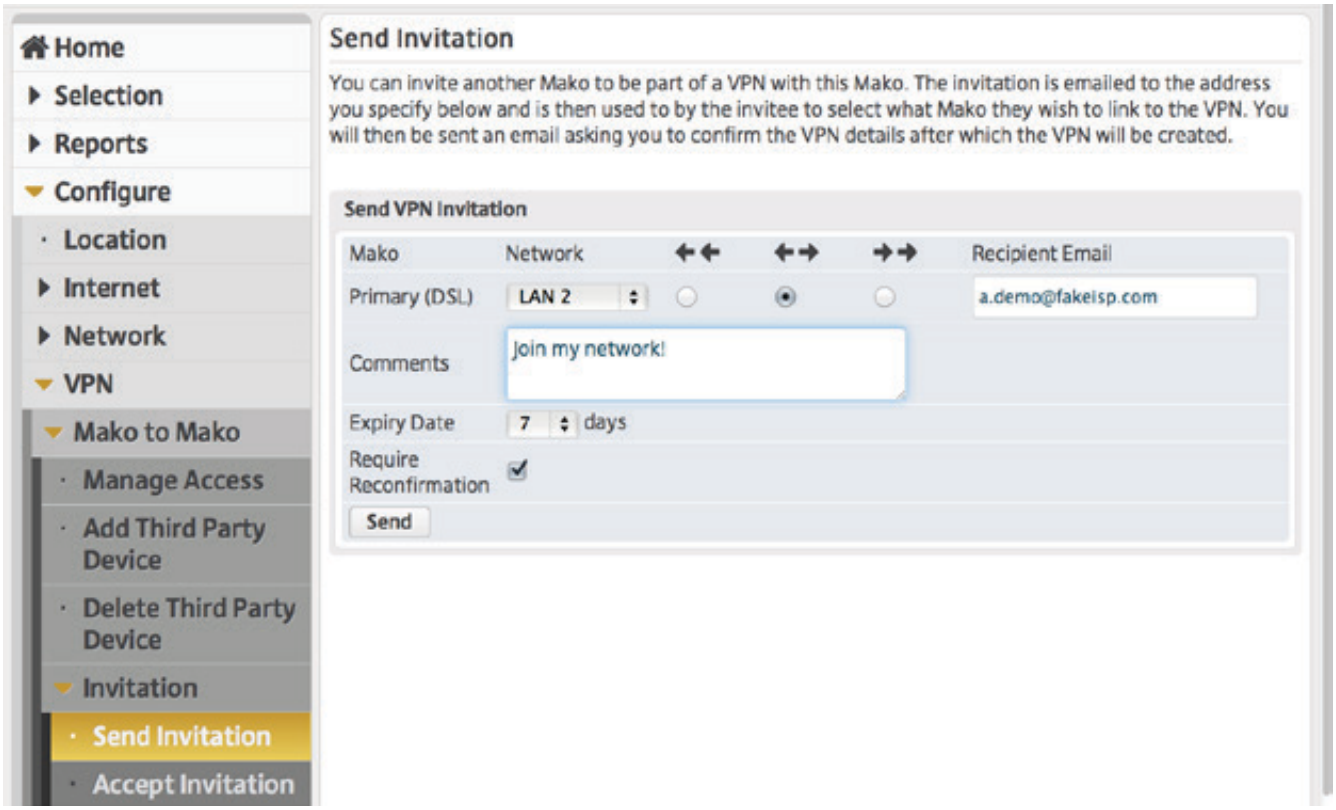
If you click **Add and Create VPN** this will take you back to the Mako to Mako VPN page, and you can continue setting up the VPN.

The third party device will appear in **Configure > VPN > Manage Access** page.

7.5 VPN > ... > Delete Third Party Device

- Select the device to be deleted from the VPN.
- **Delete** when finished.

i Mako-to-Mako VPNs have enhanced security by making use of Perfect Forward Secrecy. This is enabled by default for third-party VPNs but can be disabled.



7.6 > MAKO TO MAKO > INVITATION > SEND INVITATION

7.6 > Mako to Mako > Invitation > Send Invitation

If you wish to have a Mako to Mako VPN between your Mako and a Mako that belongs to another company, you can do so with Mako VPN Invitations.

To create a VPN between a Mako you administer and one you cannot, you need to know the email address of the other Mako's administrator.

7.6.1 Send VPN Invitation

NETWORK	Name of the Left Peer LAN over which this VPN is intended to operate.
TRAFFIC DIRECTION	← ← The Destination PCs can see those connected to your Home Mako, but not the reverse. ← → Your Home Mako PCs can see the Destination PCs and vice versa. → → The Home PCs can see those connected to your Destination Mako, but not the reverse.
RECIPIENT EMAIL	The Email address of the Right Peer device's administrator.
COMMENTS	A message about the intention and requirements surrounding the invitation (1000-character limit).
EXPIRY DATE	Number of days from sending for which the invitation is valid.
REQUIRE CONFIRMATION	This adds an extra layer of security to the invitation process: you will receive a confirmation email with another key in it that you will need to accept before the VPN is established. If you remove the check from Require Reconfirmation, this process is skipped and the VPN is established once the invited party accepts.

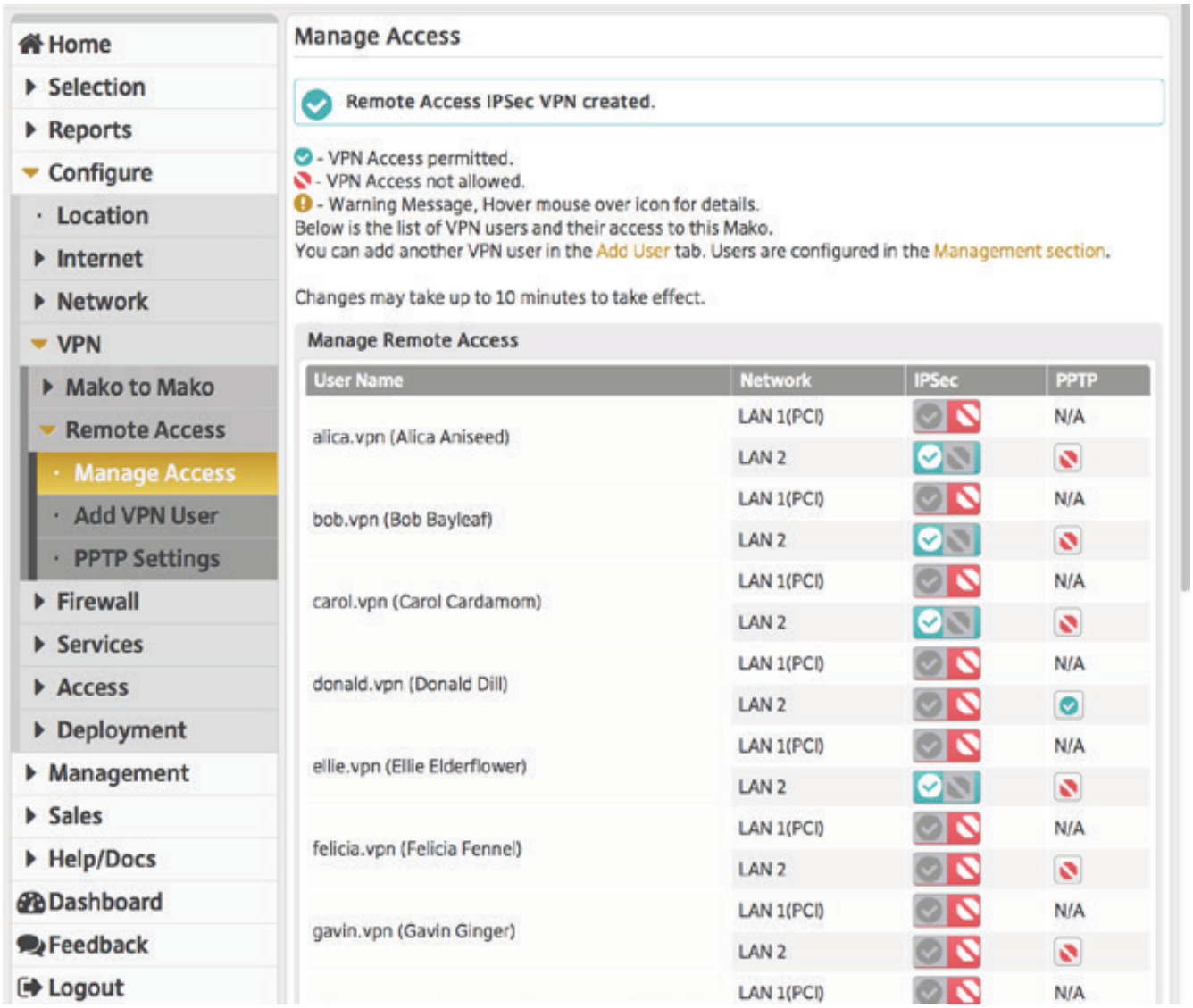
- **Send** when finished.

7.7 > Mako to Mako > Invitation > Accept Invitation

If you've received an invitation for a VPN tunnel and you wish to accept it, copy and paste the emailed key sequence, and click **Continue**.

If the **Require Reconfirmation** box was checked by the invitation Sender, then the Sender will need to complete this process. If unchecked, the VPN will be established immediately.

Once the VPN is established it will appear in the Mako to Mako VPN Manage Access list. Either party may delete the VPN at any time.



7.8 > REMOTE ACCESS > MANAGE ACCESS

7.8 > Remote Access > Manage Access

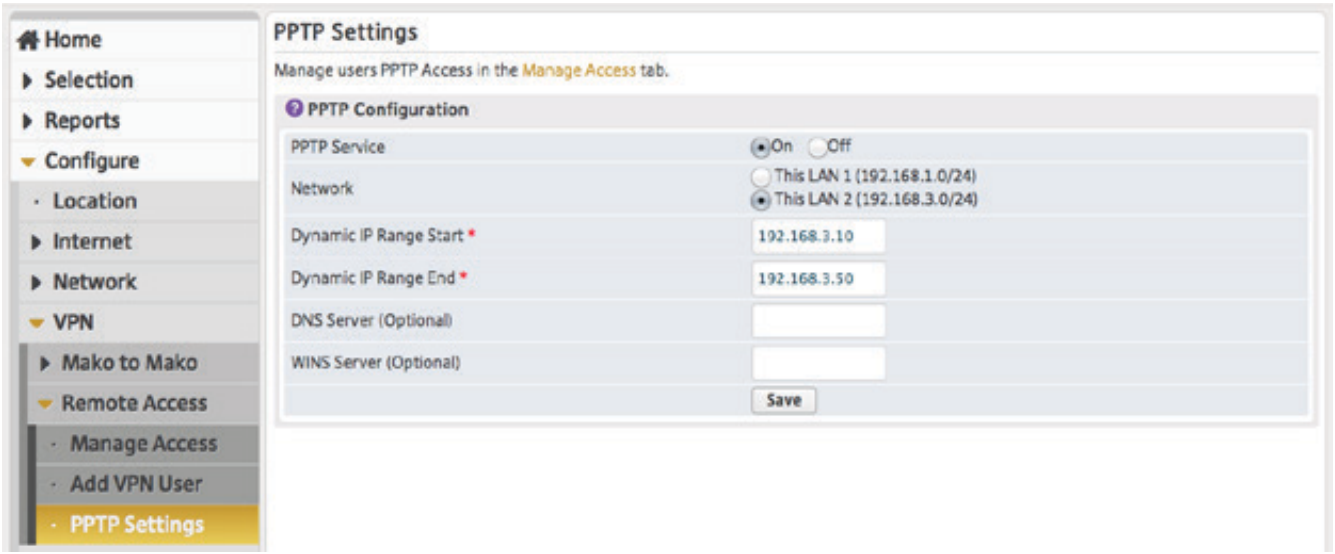
7.8.1 Manage Remote Access

USERNAME	Name of the Left Peer LAN over which this VPN is intended to operate.
NETWORK	Name of the LAN over which remote access will operate.
IPSEC	All LANs for each defined user will be listed here. : IPSec connections are permitted for this user over this LAN. : IPSec connections are denied for this user over this LAN.
PPTP	: PPTP options have not been defined. Clicking on this opens the PPTP Settings page. Once defined, the icon will change to one of the following. : PPTP connections are permitted for this user over this LAN. : PPTP connections are denied for this user over this LAN. **N/A**: Not Applicable. The LAN has been disabled for Remote Access for this user.

7.8.2 Considerations

The remote VPN user is affected by the way they connect to the Internet and the software package they use to provide a secure wrapping for their link to your office network.

7.9 > REMOTE ACCESS > ADD VPN USER



7.10 > REMOTE ACCESS > PPTP SETTINGS

7.9 › Remote Access › Add VPN User

This page creates basic user accounts for a secure private network.

- Fill in the details presented on page. All details are mandatory.
- **Add** when you've finished. i

Usernames will automatically have the **.vpn** extension appended to identify them as a VPN user and not an administrator.

You may add any number of VPN user accounts to your Mako

The Mako System is designed to support as much as **10 concurrent PPTP users per Mako**. IPSec tunnels are more flexible. See the table below.

SERIES	MAXIMUM RECOMMENDED CONCURRENT VPNS (IPSEC / PPTP)
6500 (ALL MODELS)	20 / 10 (Total: 30)
7550 (ALL MODELS)	100 / 10 (Total: 110)
8875	3000 / 10 (Total: 3010)

Once a user is configured their access can be enabled or disabled at any time.

7.10 › Remote Access › PPTP Settings

You can only enable PPTP access to one LAN.

The Mako System is designed to support as much as 10 concurrent PPTP users per Mako.

PPTP SERVICE	On / Off: Enables PPTP for this Mako. Disabling PPTP will terminate all PPTP VPNs.
NETWORK	The LAN over which PPTP will operate.
DYNAMIC IP RANGE START	Dotted decimal address. Use numbers in the range of the LAN.
DYNAMIC IP RANGE END	Dotted decimal address. Use numbers in the range of the LAN. Note: The most common Mako series, the 6500, supports 20 IPSec VPNs and 10 concurrent PPTP tunnels. Reserving more than 30 IPs (for example: 192.168.1.50 to 192.168.1.79) for VPN connections is not an optimal configuration.
DNS SERVER (OPTIONAL)	If required, enter the address of a DNS here.
WINS SERVER (OPTIONAL)	If you use Microsoft's Windows Internet Name Service, enter the address of a DNS here.

- **Save** when finished.

---

i To delete a user: Management > User > Manage [username] > Access Control, then **delete user.**

8 Configure › Firewall

8.1 Overview

The default security configuration for a Mako is to block all communications initiated from the Internet from entering your networks, while all communications initiated from the office network can access the Internet. You may 'call out', but no-one may 'call in'.

This means that users on your Mako-protected networks can send and receive their email, browse the World Wide Web, and access all other Internet-based services, while the firewall ensures that none of their PCs are visible to the Internet.

- Changes to permissions which deny access tend to **improve** network security.
- Changes which allow access tend to **weaken** network security.

Changes to permissions should therefore specify the permitted access as narrowly as possible to minimize risk of unapproved intrusion.

8.1.1 Rule Hierarchy

The CMS allows you to set up rules that allow inbound and outbound traffic to your system, but sometimes these rules might be in conflict, which is why the CMS needs a rule hierarchy. **Rules at the top of a list have precedence**: the top-most rule is applied first, followed by the next highest, and so on.

8.1.2 Delete, Edit, View or Promote an Option

- In Existing Rules section, click ⊗, ⚙, 👁 or ↑.

8.1.3 › Inbound, Outbound, Intranet, VPNs

These CMS pages relate to the firewall rules that permit communications to be initiated from the Internet into your local networks by a remote host computer.

It is important to understand that for **Inbound** access – whether it's for general Inbound traffic from the Internet, intranet or even from internal Mako-to-Mako traffic – the rules place some responsibility for security of the network onto the target local network PC or server. The firewall will permit all communications matching the access rules.

Other than this, Inbound, Outbound, Intranet and VPN traffic all use near-identical features in setting rules: they are provided in separate pages for ease of use. [i], [ii]

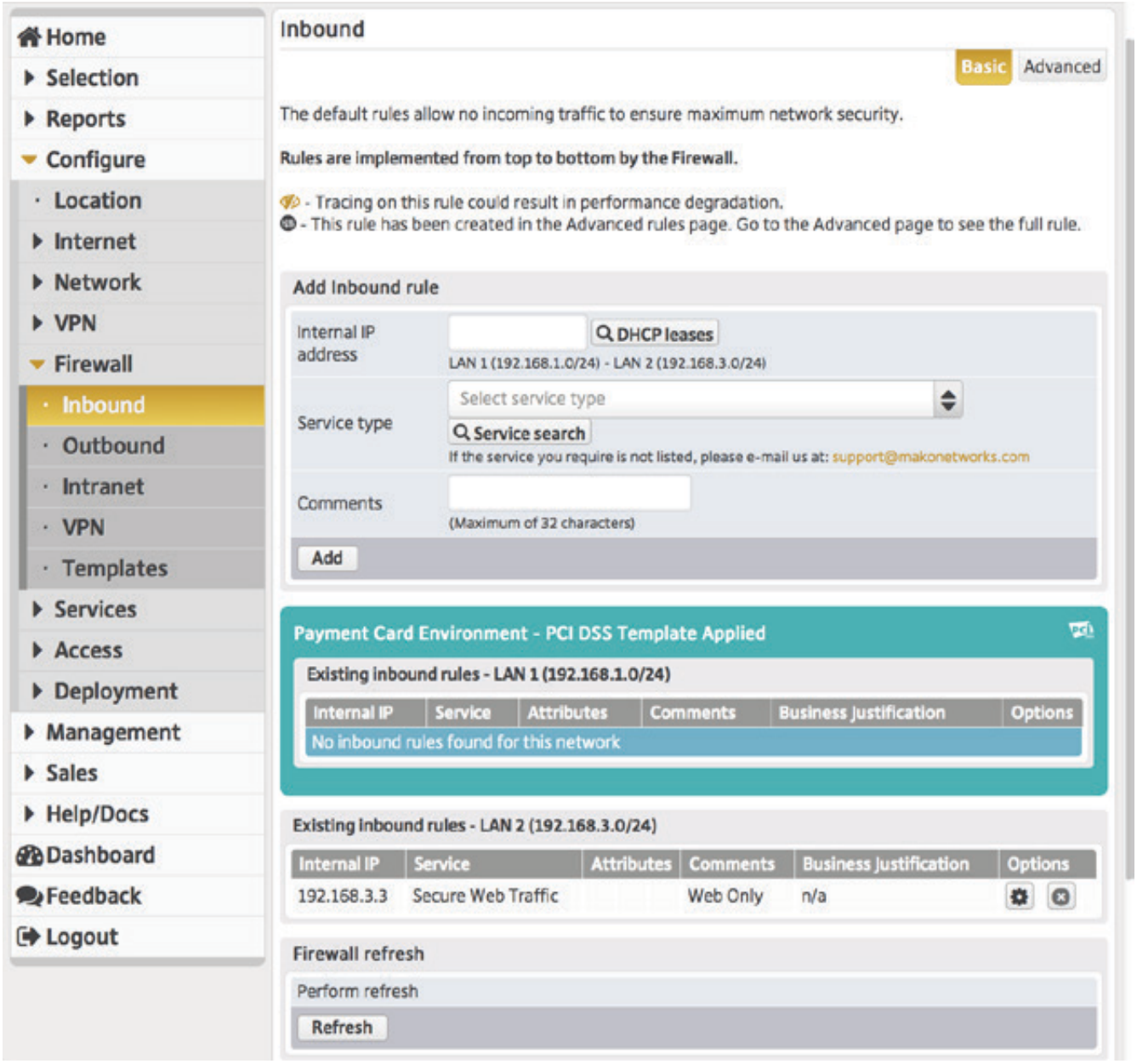
8.1.4 Trace Logging

Trace logging allows you to trace individual IP connections allowed and denied through the firewall. This is used to help track down firewall related connection problems, and is displayed in the Reports Syslog section. Generally, traffic doesn't need to be traced unless you are tracking down a specific rule issue. Tracing will reduce the level of performance offered.

---

i If the local PC or server is not itself secure, then other PCs in the office network can be exposed.

ii Each Mako has at least two isolated LANs built-in, but these LANs can be bridged to share networks. To help keep systems as secure as possible, ensure that targeted PCs on the designated LAN have the appropriate security-related updates applied to their software.



8.2 > INBOUND (BASIC)

8.2 › Inbound (Basic)

This is where firewall rules for incoming traffic to the Mako's LAN are set. By default, the Mako is set to **Deny All Access** initiated by hosts from the Internet. i

8.2.1 Add Inbound Rule

INTERNAL IP ADDRESS The Internal IP Address to which the rule will be applied. Often this will be the address of your Mako. Below the field is are the Mako's LANs for convenience.

DHCP leases

This button creates a pop-up, listing the DCHP Leases created under **Configure > Network >** DHCP Leases. Selecting a DHCP lease will copy it into the Internal IP Address field.

SERVICE TYPE Several services, such as FTP, POP, IMAP and web content happen over specific ports. Some services use ranges of ports. You may type in either a port number or a service description in this field to reserve an appropriate port for this incoming traffic.

Service search

This button creates a pop-up form where you can enter a name or port to search with. Clicking on the resulting links enters the link into the **Service type** field.

COMMENTS While optional, this name will allow you to search by terms in this comment, and is useful to know when diagnosing rule clashes.

- Click **Add** when finished.

The page will refresh and the latest rule will be added as the last rule to be executed in the list.

i Tracing on this rule could result in performance degradation.

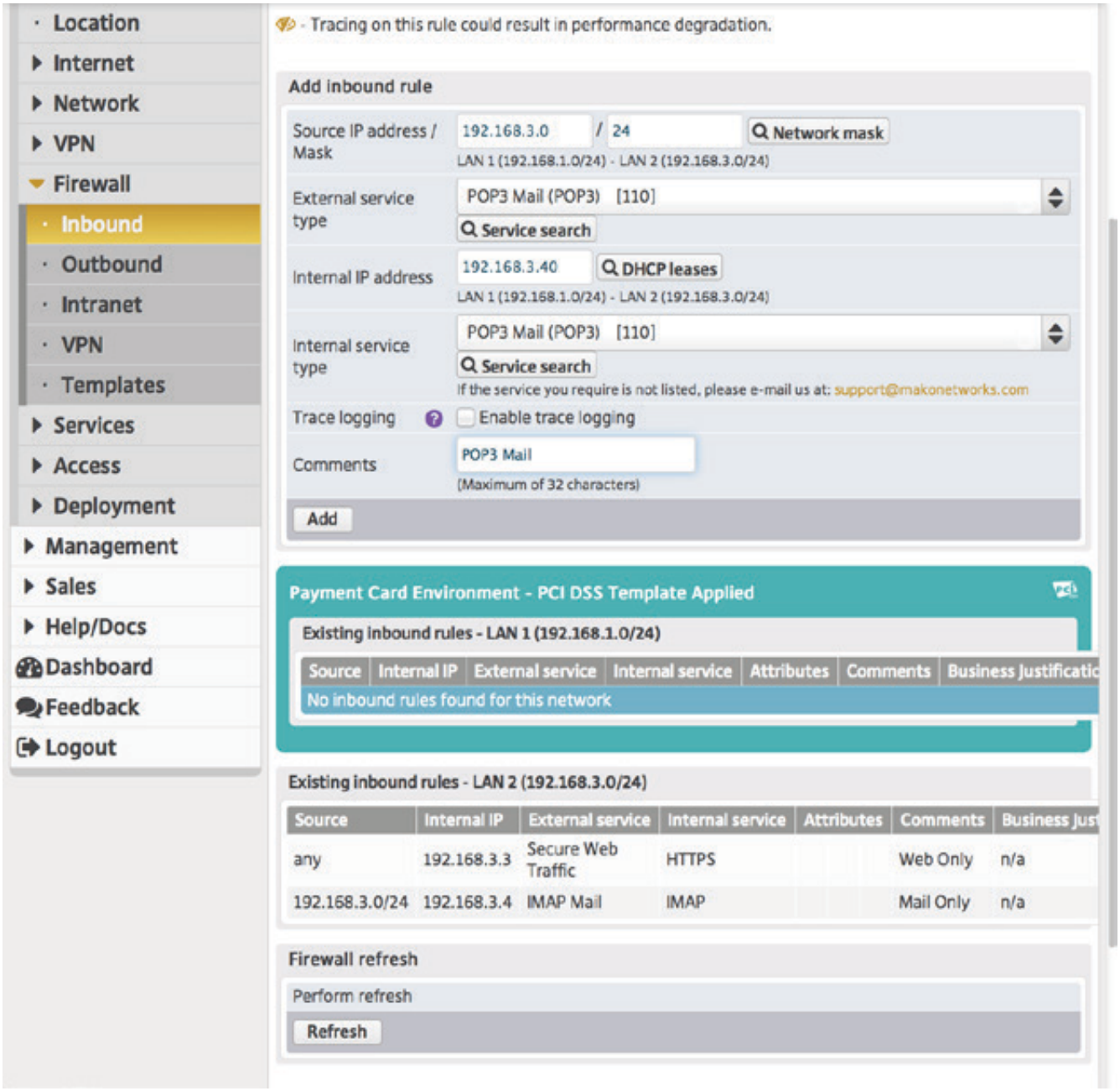
8.2.2 Existing inbound rules

The forms below the entry field list the current rules, grouped by LAN.

INTERNAL IP	The IP of the LAN device to which the traffic is addressed.
SERVICE	The name/port listing associated to the service being processed.
ATTRIBUTES	Three icons may be listed here. : indicates the class of LAN device: Generic, Computer, Printer, Payment terminal, Storage. Click to edit the attributes. : indicates if the rule was created in the Advanced section. : indicates if the rule is being trace-logged (If you see this icon, trace logging is ON.)
COMMENTS	While optional, this name will allow you to search by terms in this comment, and is useful to know when diagnosing rule clashes.
BUSINESS JUSTIFICATION	**PCI ONLY**. If this LAN has the PCI DSS Template applied, the business justification is listed.
OPTIONS	: Allows you to edit the Inbound rule. : Allows you to delete the Inbound rule. : Allows you to promote the Inbound rule. The ordering of firewall rules is important, as they're applied sequentially.

Refresh

This button forces the changes to apply immediately to your Mako.



8.3 INBOUND > ADVANCED

8.3 Inbound > Advanced

Advanced firewalls differ in that they add more details about the ports and services being specified.

SOURCE IP ADDRESS/MASK The IP of the LAN device the traffic is addressed, and a range, in CIDR notation, of addresses that apply to this rule.

PCI DSS Template applied: Clicking **Add** will refresh the page and ask you to re-enter your password and the Business Justification for adding the new rule. (satisfying requirements 1.1.5, 1.2.1 & 1.3 of the PCI DSS.)

EXTERNAL SERVICE TYPE Several services, such as FTP, POP, IMAP and web content happen over specific ports. Some services use ranges of ports. You may type in either a port number or a service description in this field to reserve an appropriate port for this incoming traffic.

Service search

This button is most useful for searching ranges of port addresses. It creates a pop-up form where you can enter a name or port to search with. Clicking on the resulting links enters the link into the **Service type** field.

INTERNAL IP ADDRESS The Internal IP Address to which the rule will be applied. Often this will be the address of your Mako. Below the field is are the Mako's LANs for convenience.

DHCP leases

This button creates a pop-up, listing the DCHP Leases created under **Configure > Network > DHCP Leases**. Selecting a DHCP lease will copy it into the Internal IP Address field.

INTERNAL SERVICE TYPE This maps the External Service/Port to a Service/Port used internally. This allows several distinct streams of port traffic to be managed by a uniform, internally-defined schema.

Service search

This button creates a pop-up form where you can enter a name or port to search with. Clicking on the resulting links enters the link into the **Service type** field.

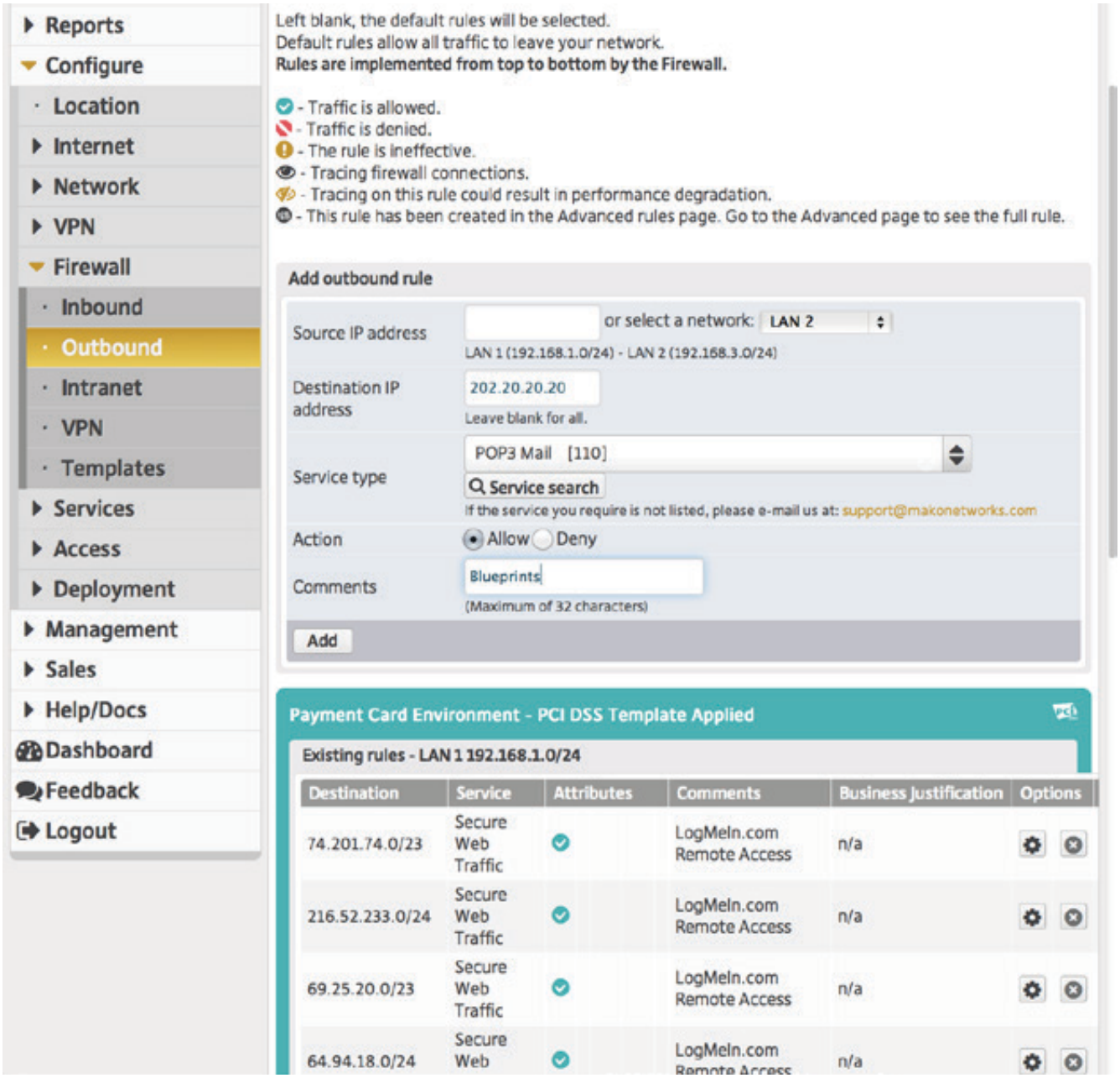
TRACE LOGGING Enables trace logging. *Trace Logging...*

COMMENTS While optional, this name will allow you to search by terms in this comment, and is useful to know when diagnosing rule clashes.

- **Add** when finished.

8.3.1 Existing Inbound Rules

SOURCE	The source IP Address of the traffic that will be processed by this rule.
INTERNAL IP	The IP of the LAN device to which the traffic is addressed.
EXTERNAL SERVICE	The name associated to the service being processed.
INTERNAL SERVICE	The name associated to the service to which the external service will be mapped.
ATTRIBUTES	Three icons may be listed here.  : indicates the class of LAN device: Generic, Computer, Printer, Payment terminal, Storage. Click to edit the attributes.  : indicates if the rule was created in the Advanced section.  : indicates if the rule is being trace-logged (If you see this icon, trace logging is ON.)
COMMENTS	While optional, this name will allow you to search by terms in this comment, and is useful to know when diagnosing rule clashes.
OPTIONS	 : Allows you to edit the inbound rule.  : Allows you to delete the inbound rule.  : Allows you to promote the inbound rule. The ordering of firewall rules is important, as they're applied sequentially.



8.4 > OUTBOUND (BASIC)

8.4 › Outbound (Basic)

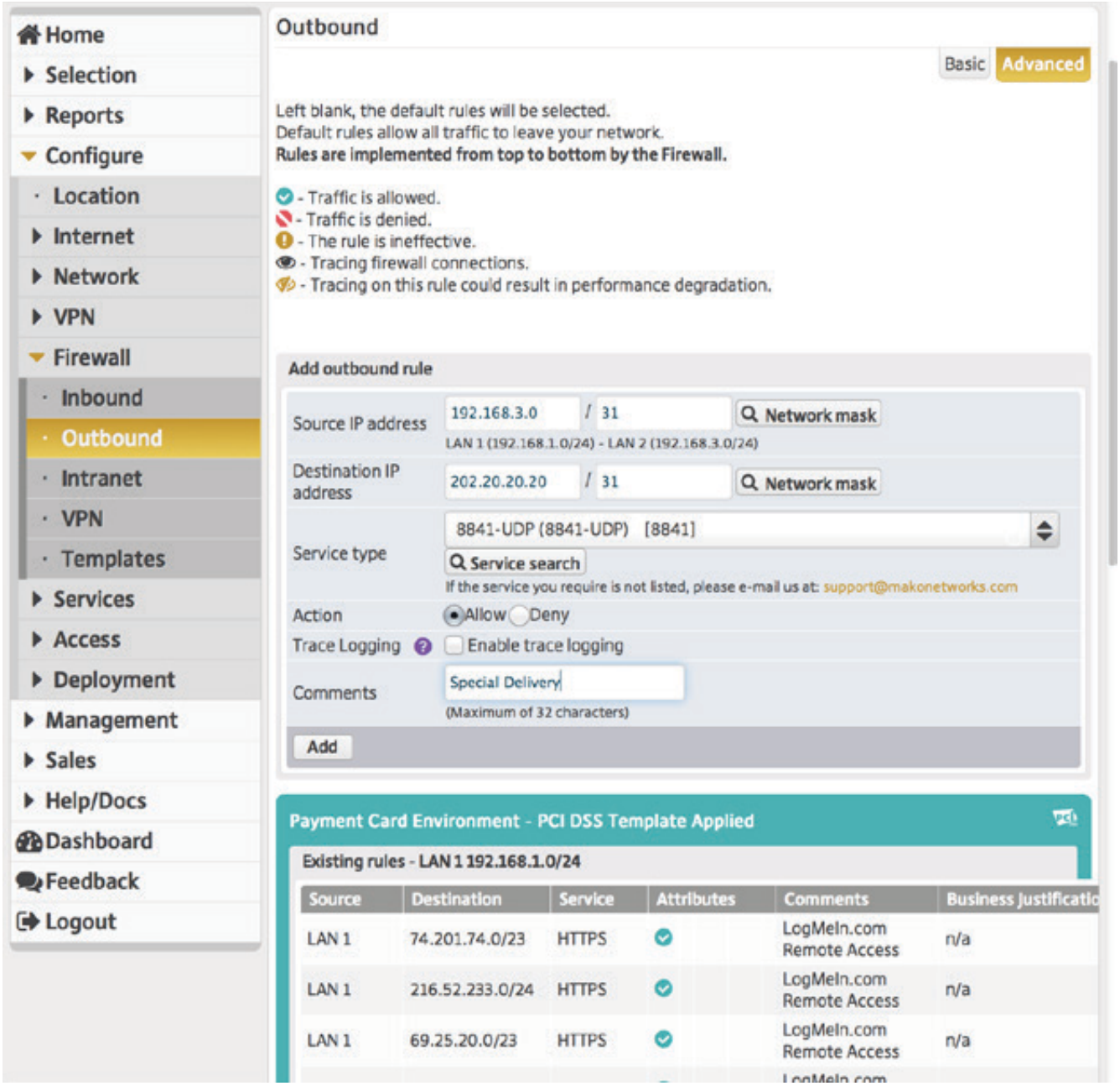
By default, outbound traffic is set to **Allow** all traffic to leave your network, or may leave your computer to another computer on your network. A firewall will ensure that communications are only initiated by PCs on the Mako's local network, however once established these communications are bi-directional.

8.4.1 Add outbound rule

SOURCE IP ADDRESS	The IP of the LAN device to which the traffic is addressed, or simply select a network for which the rule will apply.
DESTINATION IP ADDRESS	The specific IP this rule is for (leave bank for all IP addresses).
SERVICE TYPE	The contextual search field will filter results as you type. You may enter port numbers, service descriptions or substrings to find and select results. Service search This button is most useful for searching ranges of port addresses. It creates a pop-up form where you can enter a name or port to search with. Clicking on the resulting links enters the link into the **Service type** field.
ACTION	Select whether qualifying traffic is to be allowed out, or denied from being sent.
COMMENTS	While optional, this name will allow you to search by terms in this comment, and is useful to know when diagnosing rule clashes.

8.4.2 Existing rules - LAN [LAN RANGE]

DESTINATION	The IP of the LAN device to which the traffic is addressed.
SERVICE	The name/port listing associated to the service being processed.
ATTRIBUTES	Three icons may be listed here. : indicates this rule either allows or denies outgoing traffic. : indicates if the rule was created in the Advanced section. : indicates the rule is being trace-logged. *Trace Logging...*
COMMENTS	Additional description of the rule.
BUSINESS JUSTIFICATION	**PCI DSS template**: If this LAN has the PCI DSS template applied, the business justification is listed. (satisfying requirements 1.1.5, 1.2.1 & 1.3 of the PCI DSS.)
OPTIONS	: Allows you to edit the outbound rule. : Allows you to delete the outbound rule. : Allows you to promote the outbound rule. The ordering of firewall rules is important, as they're applied sequentially.



8.5 > OUTBOUND (ADVANCED)

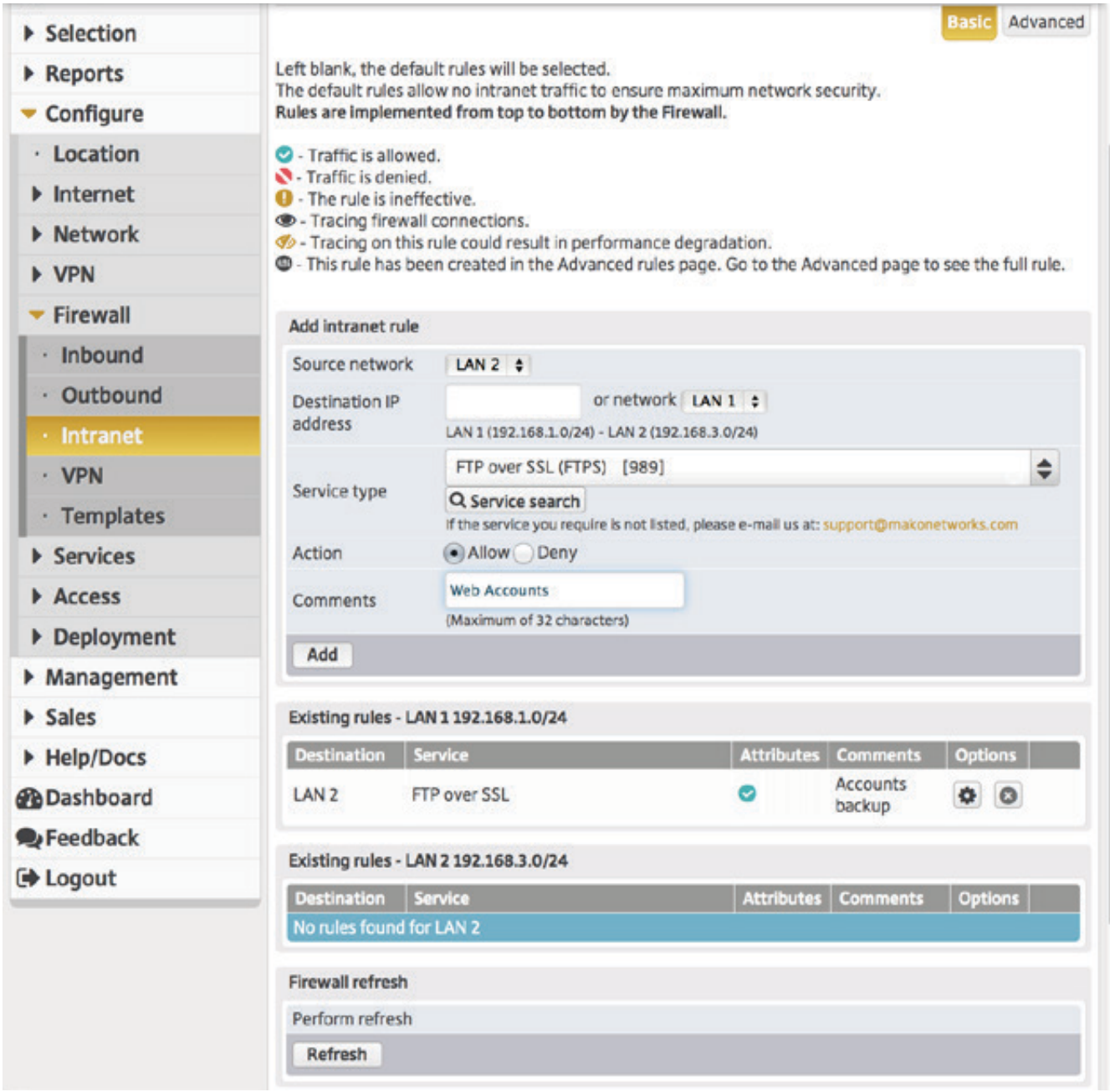
8.5 › Outbound (Advanced)

8.5.1 Add outbound rule

SOURCE IP ADDRESS	The IP of the LAN device to which the traffic is addressed, or simply select a network for which the rule will apply.
DESTINATION IP ADDRESS	The specific IP this rule is for (leave bank for all IP addresses).
SERVICE TYPE	The contextual search field will filter results as you type. You may enter port numbers, service descriptions or sub-strings to find and select results.  This button is most useful for searching ranges of port addresses. It creates a pop-up form where you can enter a name or port to search with. Clicking on the resulting links enters the link into the **Service type** field.
ACTION	Select whether qualifying traffic is to be allowed out, or denied from being sent.
COMMENTS	While optional, this name will allow you to search by terms in this comment, and is useful to know when diagnosing rule clashes.

8.5.2 Existing rules - LAN [LAN RANGE]

DESTINATION	The IP of the LAN device to which the traffic is addressed.
SERVICE	The name/port listing associated to the service being processed.
ATTRIBUTES	Three icons may be listed here. : indicates this rule either allows or denies outgoing traffic. : indicates if the rule was created in the Advanced section. : indicates the rule is being trace-logged. *Trace Logging...*
COMMENTS	Additional description of the rule.
BUSINESS JUSTIFICATION	**PCI DSS template**: If this LAN has the PCI DSS template applied, the business justification is listed. (satisfying requirements 1.1.5, 1.2.1 & 1.3 of the PCI DSS.)
OPTIONS	: Allows you to edit the outbound rule. : Allows you to delete the outbound rule. : Allows you to promote the outbound rule. The ordering of firewall rules is important, as they're applied sequentially.



8.6 > INTRANET (BASIC)

8.6 › Intranet (Basic)

The **Intranet** pages (Basic and Advanced) are rules for traffic within a private network and treat Inbound and Outbound traffic as the same. i In terms of function, the Intranet (Basic) page differs from Inbound and Outbound Basic pages only in the addition of the Source Network and 'or network' fields.

There are a few occasions when an Internet-based host needs to initiate communications with a PC on the office network. A common example is when a mail server is located in the office network, inside the firewall. It's often necessary for the mail server to receive incoming connections from mail hosts on the Internet, and this requires an access path through the firewall to be configured.

SOURCE NETWORK	The IP of the LAN device to which the traffic is addressed, or simply select a network for which the rule will apply.
DESTINATION IP ADDRESS	The specific local IP this rule is for, or you my use the **or network** field to select one of your local networks.
SERVICE TYPE	The contextual search field will filter results as you type. You may enter port numbers, service descriptions or substrings to find and select results. Service search This button is most useful for searching ranges of port addresses. It creates a pop-up form where you can enter a name or port to search with. Clicking on the resulting links enters the link into the **Service type** field.
ACTION	Select whether qualifying traffic is to be allowed out of this network, or denied from being accepted by this network.
COMMENTS	While optional, this name will allow you to search by terms in this comment, and is useful to know when diagnosing rule clashes.

- **Add** when finished.

i It isn't recommended to modify the default settings, as you could reduce the security provided by having separate networks.

8.6.1 Existing rules

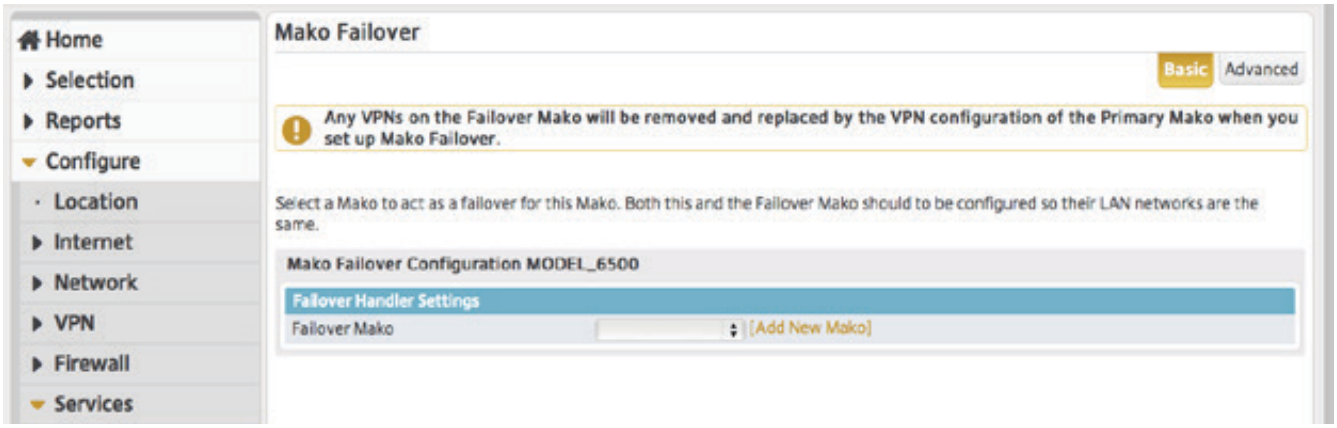
DESTINATION	The IP of the LAN device to which the traffic is addressed.
SERVICE	The name/port listing associated to the service being processed.
ATTRIBUTES	Three icons may be listed here. : indicates this rule either allows or denies outgoing traffic. : indicates if the rule was created in the Advanced section. : indicates the rule is being trace-logged. *Trace Logging...*
COMMENTS	Additional description of the rule.
BUSINESS JUSTIFICATION	**PCI DSS template**: If this LAN has the PCI DSS template applied, the business justification is listed. (satisfying requirements 1.1.5, 1.2.1 & 1.3 of the PCI DSS.)
OPTIONS	: Allows you to edit the outbound rule. : Allows you to delete the outbound rule. : Allows you to promote the outbound rule. The ordering of firewall rules is important, as they're applied sequentially.

If your ISP provides you with multiple public IP addresses you may specify a public IP address that the inbound rule refers to. This is useful if you want to have multiple rules to the same port on different internal PCs. i

8.6.2 VPN Specifics

Before you can add rules to a Virtual Private Network firewall, you must create the VPN in the separate VPN Section. VPNs have a specific name and traffic direction.

i If your ISP doesn't provide you with multiple public IP addresses you will not see the Target IP address drop-down. This is likely to be the case for most ISPs.



9.1 > MAKO FAILOVER

9 Configure › Services

All Makos handle several optional services. Please check our support address for the latest available.

Documentation for Services that require an additional licence can be downloaded in PDF format from the Help/Docs section of the CMS.

9.1 › Mako Failover

This page concerns Mako-to-Mako Failover. A second Mako (called the 'Failover Handler') connects with a Primary Mako over a LAN in a 'heartbeat' configuration, so that if the Primary Mako goes down the Failover Handler handles the site's network administration.

Mako-to-Mako Failover is a High Availability option for clients for whom uninterrupted connectivity is a vital requirement. The Secondary Mako is recommended to run on a separate power supply, using a different ISP from the Primary.

Failover conditions, and the time the Makos take to failover and failback, are evaluated from several metrics. But generally the failover process is triggered by the primary Mako losing its WAN connection, losing a LAN connection or suffers an electrical outage. The failover process takes around 5 minutes. [i]

9.1.1 Configurations transferred on Failover

Settings for all Makos are stored in the cloud-based CMS. If the Primary Mako goes down, the Failover Handler retrieves most of the Primary's settings from the CMS, including:

WLANs **VLANs** **VPNs** **MakoMail**

DHCP Leases **Static Routes** **Dynamic DNS** **Mako Guardian**

Certain administrative labels (LAN names, LAN IDs, Allow Pingetc.) may be changed on the Failover Handler without affecting the failover configuration.

9.1.2 Configurations not transferred on Failover

Some settings will not carry over, due to the IP Address-specific nature of devices on the Internet.

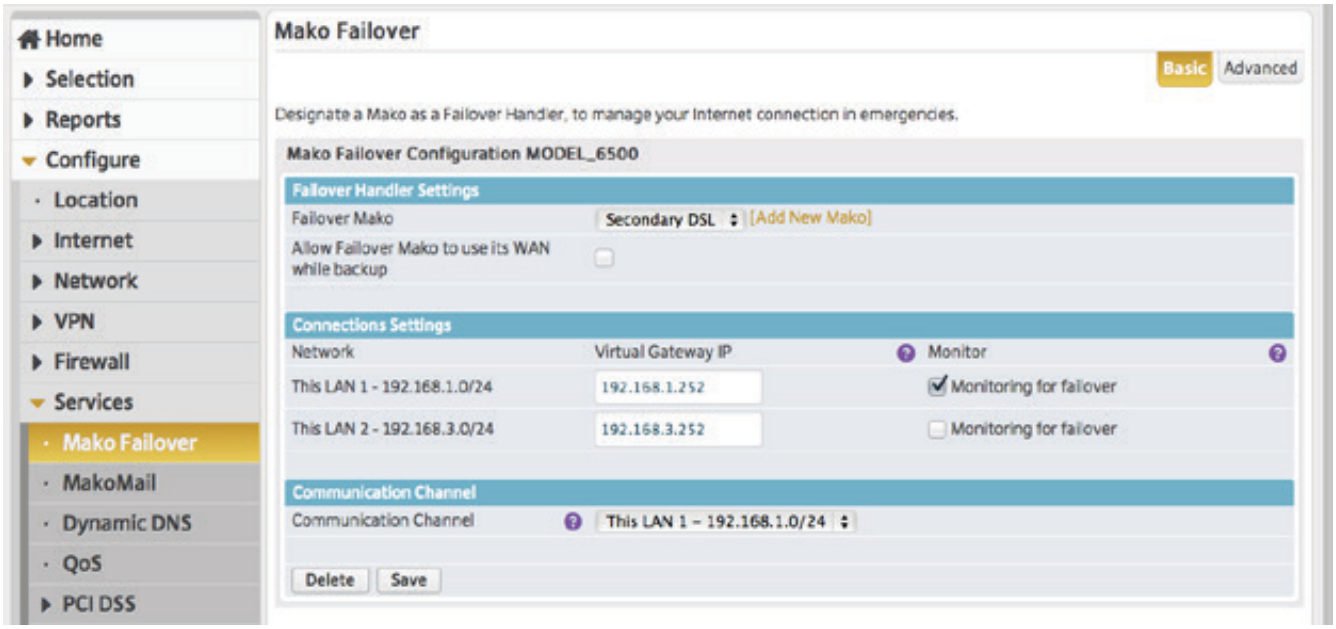
Internet connection settings **Specific network ranges**

Firewall rules [ii]

---

[i] We recommend configuring both the Primary and Failover Makos BEFORE you enable Mako Failover. For Failover to work, your Failover Handler needs to be on the same subnet as the Primary.

[ii] Firewall rules that exist on the Failover Handler will remain on the Failover Handler. If a failover event occurs, firewall rules are not cleared nor overwritten.



9.2 CONFIGURING MAKO-TO-MAKO FAILOVER (BASIC)

9.2 Configuring Mako-to-Mako Failover (Basic)

- With the Primary Mako selected within the CMS, select the Mako you would like to use as the Failover Handler. i

Once Selected, a form will appear.

9.2.1 Failover Handler Settings

FAILOVER MAKO	Choose the Mako to be used as the Failover Handler.
ALLOW FAILOVER MAKO TO USE ITS WAN WHILE BACKUP	In an ideal situation, the Failover Handler is redundant, spending most of its life polling the Primary to see if it needs to take over. But if you wish, the Failover Handler may be used as an independent router during downtime. If/when a failover event happens the network will switch to using the Failover Handler's WAN and import the Primary's settings.

9.2.2 Connections Settings

NETWORK	This column lists the IP Addresses for the Primary Mako.
VIRTUAL GATEWAY IP	This column suggests an IP Address over which the two Makos may talk.
MONITOR	This column's checkboxes allows a failover event to occur if the checked LAN goes down. If neither box is selected, a failover event occurs only if the Primary WAN goes down (or a loss of power to the Primary Mako). Should a checked LAN go down, the Failover Handler will run both LANs.

9.2.3 Communication Channel

COMMUNICATION CHANNEL	This channel is used solely for Failover communications and internal Mako negotiation over which Mako is best for continuing service. This is often left at the default address.

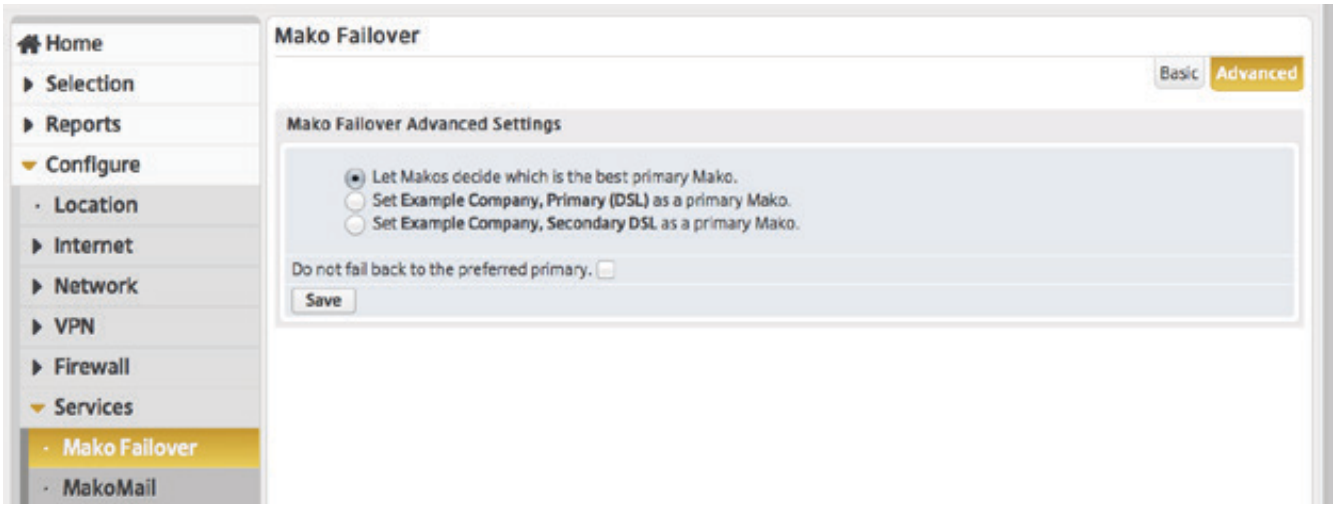
- Click **Save**.

9.2.4 Considerations

For Mako-to-Mako Failover to be configured:

- Ensure each LAN operates over the same subnet. If the refreshed page shows red backgrounds in the Connection Settings area, your Makos are on different subnets. Typically, many choose the 192.168.x.y subnet schema: in this case, ensure the Virtual Gateway IP x value is the same for each LAN 1 – for example, 1 – and the same for each LAN 2 –for example, 2. Each subnet must be different.
- Only Makos of the same series and the same number of LANs may be in a Failover configuration. So 7550s may be Failover pairs; 8875s may be Failover pairs; 6500-E–to–6500-A2 may be Failover pairs, but

i Or click **Add New Mako**, and configure a new one.



9.2.5 FAILOVER > ADVANCED

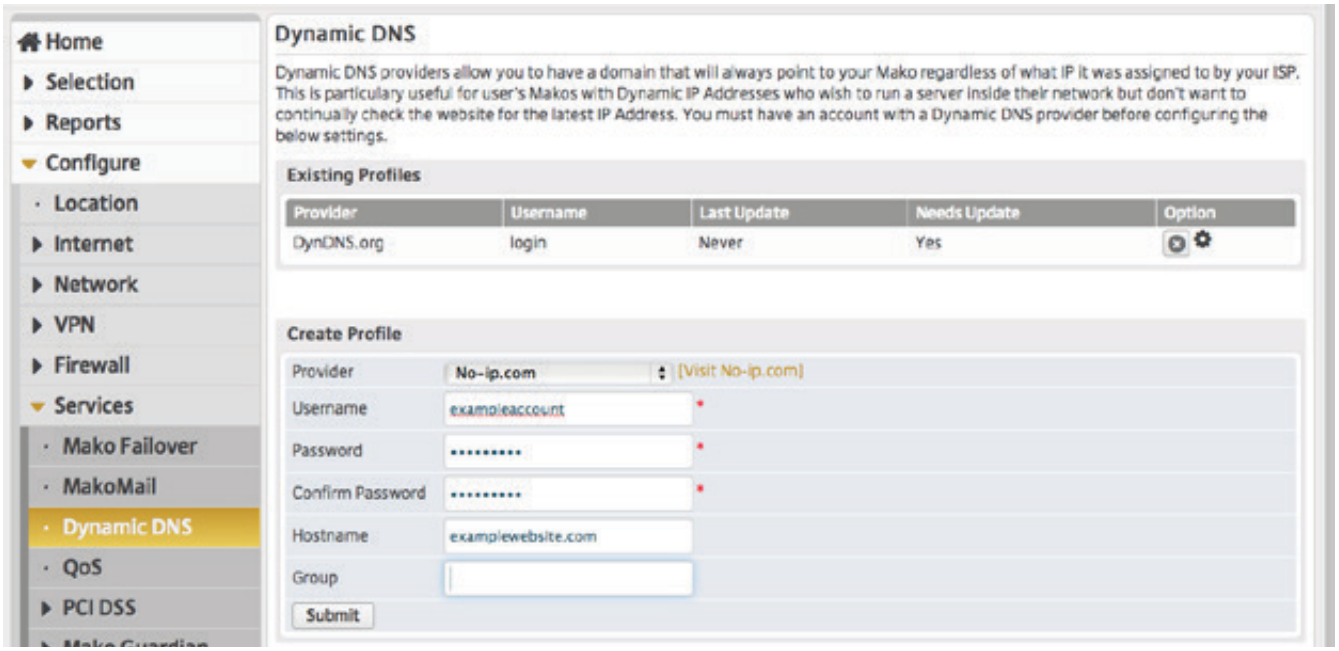
the 6500-M may not be used with 6500-Es or 6500-A2s as the M-model has four LANs, while the others have two.

9.2.5 Failover > Advanced

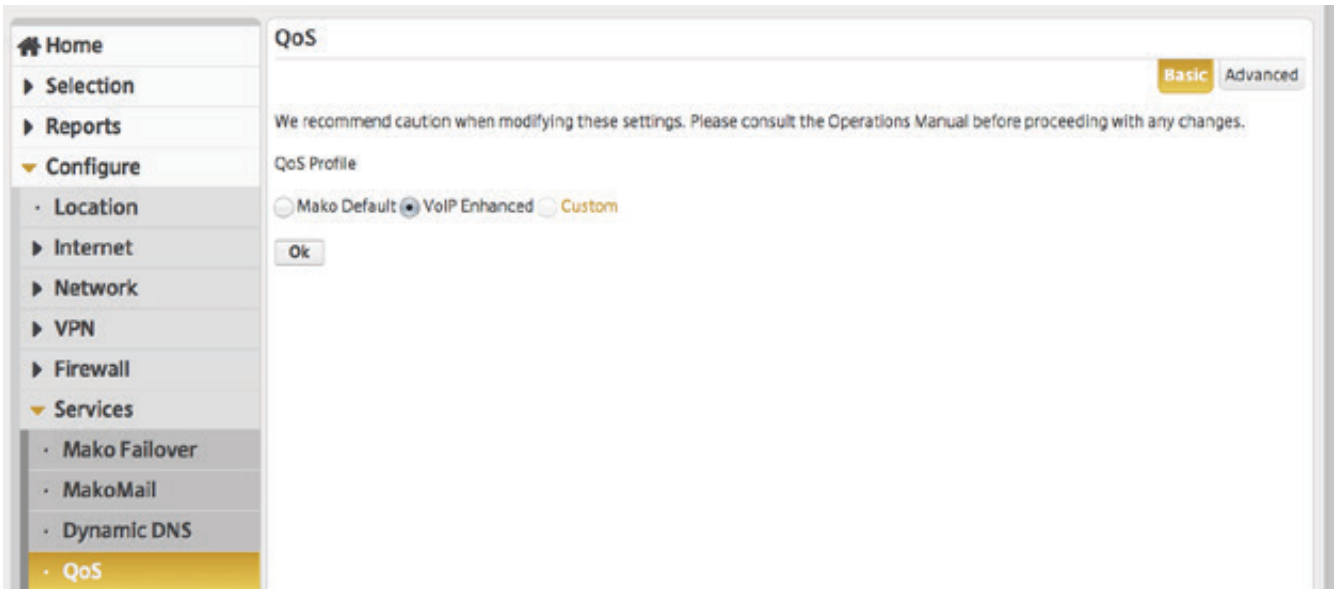
While in the failover state, the Primary Mako could be fixed, or re-establish a stable connection to the Internet. If this happens you can choose how your network handles this situation. i

- **Let Makos decide which is the best primary Mako:** If the Primary is found to be in a stronger state of health, the Primary will resume its network management role.
- **Set [Primary Mako Name] as a primary Mako:** Even if the Failover Handler is found to be in a stronger position, the Primary will resume its network management role.
- **Set [Failover Handler Name] as a primary Mako:** Even if the Primary Mako is found to be in a stronger position, the Failover Handler will continue its new network management role.
- **Do not fail back to the preferred Primary:** the first three options involve the Makos negotiating over which is the healthiest to continue managing the network. This switch effectively turns off failback altogether, allowing the customer to do a manual failback (if desired) at a time of their own choosing.
- Click **Save**.

i Determining Mako failback conditions can take around an hour. This negotiation takes place between the two Makos. Once the decision has been evaluated and the Primary is required to take back its network, failback normally takes between 3 and 10 minutes.



9.3 > DYNAMIC DNS



9.4 > QOS > BASIC

9.3 › Dynamic DNS

Dynamic DNS providers allow you to have a domain that will always point to your Mako regardless of what IP it was assigned to by your ISP.

This is particularly useful for user's Makos with Dynamic IP Addresses who wish to run a server inside their network but don't want to continually check the website for the latest IP Address. Dynamic DNS requires a free subscription to one of two third-party Dynamic DNS providers, DynDNS.org or no-ip.com. i

9.3.1 Create Profile

PROVIDER	Select your Dynamic DNS provider.
USERNAME	The username you registered with your Dynamic DNS provider account.
PASSWORD/ CONFIRM PASSWORD	Enter the password for your Dynamic DNS provider account.
HOSTNAME	Enter the hostname.
WILDCARD (DYN.COM)	A wildcard domain is one where all subdomains share the same set of files. Enter your wildcard here.
MAIL EXCHANGER (DYN.COM)	Enter your mail server address here, either dotted-decimal format or domain.suffix.
BACKUP MX	Enter your mail server back-up address here.

9.4 › QoS › Basic

Quality of Service (QoS) allows you to prioritize different types of Internet traffic and specify minimum outbound bandwidth allocations. QoS can be used to improve the quality of such services as VOIP traffic, by ensuring there is always bandwidth reserved for it, and that it has priority over less demanding services such as web browsing.

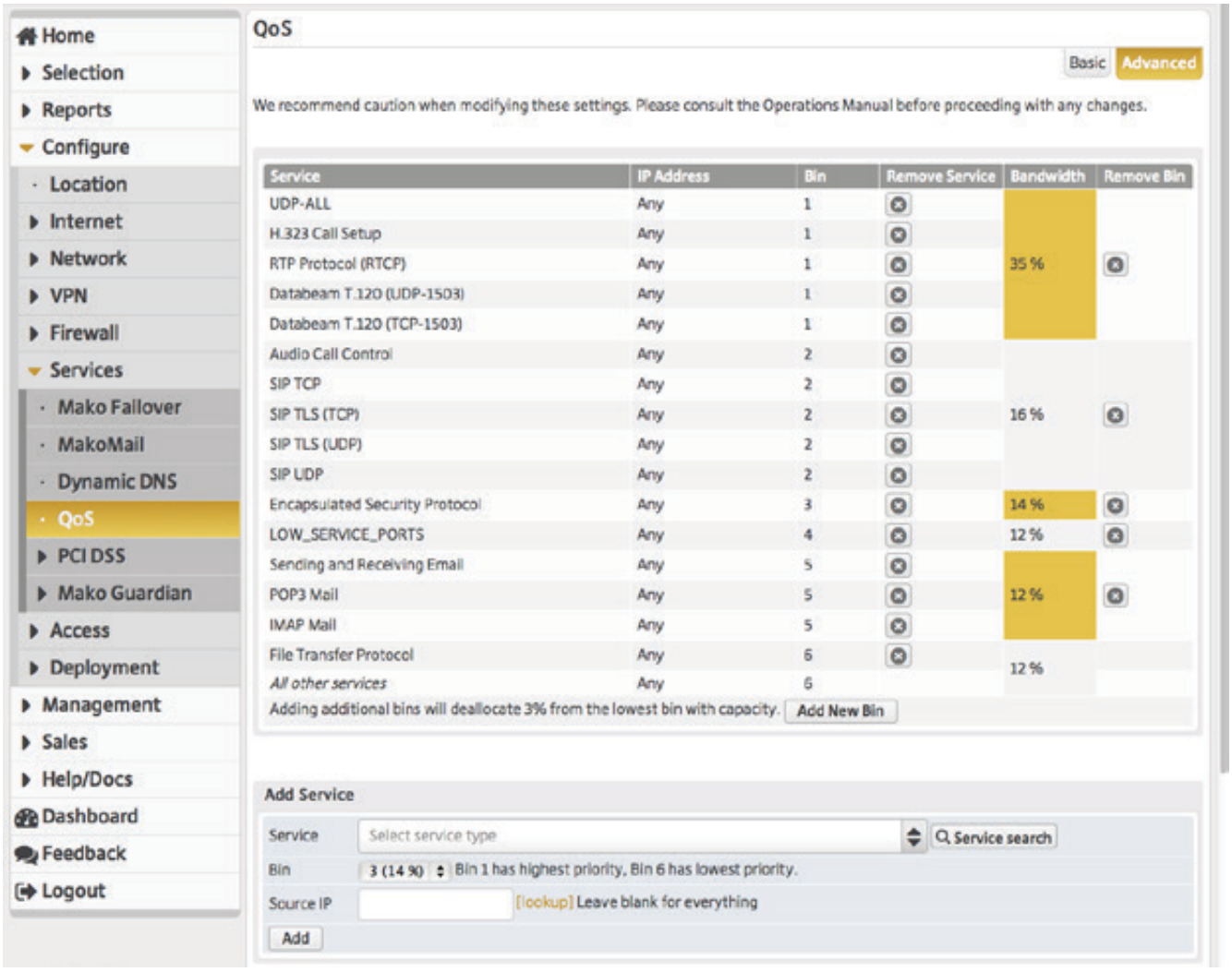
The Mako default setting is recommended for most users. This setting allocates bandwidth reservations to the most common Internet applications and traffic types.

The VoIP Enhanced setting guarantees VoIP traffic approximately 33% of your upstream bandwidth. Use this setting if you require enhanced VoIP quality and reliability.

- Select a QoS Profile setting

OK when finished.

i Your reseller neither endorses nor guarantees the services provided by either of these parties. We provide the Dynamic DNS service as a convenience to the users of its products.



9.5 > QOS > ADVANCED

9.5 > QoS > Advanced

QoS Advanced is for more detailed control over upstream service priorities.

The upstream bandwidth is broken into segments, called **bins**. Selected services are placed in these bins and given priority by the bin number (Bin 1 has top priority).

The percent value for each of the bins indicates the minimum guaranteed upstream bandwidth to be shared by all the services using that bin. If some upstream bandwidth is unused, it can be temporarily borrowed from other bins until the bin needs the bandwidth.

All services that belong to a particular bin share its bandwidth. Important or high priority services should be placed in a bin with no more than two other services to ensure the bandwidth for the bin is not shared between too many services.

The total bandwidth allocation across all bins adds up to 100%. Services that are not allocated to a bin use the last bin by default. Adding too many bins can seriously degrade performance. Services that are not allocated to a bin use the last bin by default. i

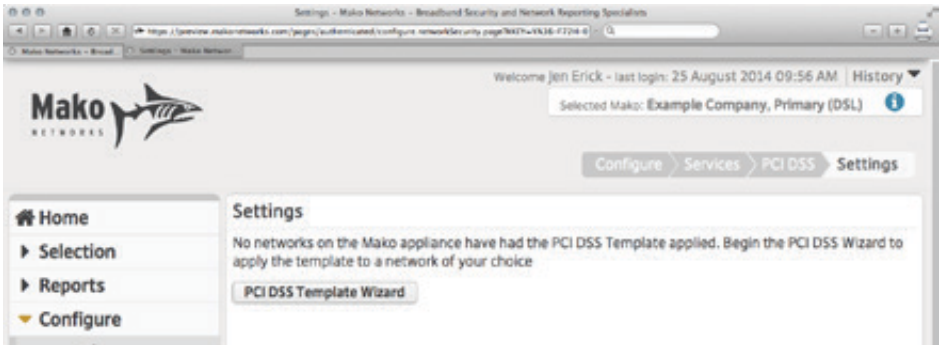
SERVICE	The Internet service/protocol contained within a bin.
IP ADDRESS	The source IP address (or Any) on which the priority is active.
BIN	The bin number. 1 is top priority.
REMOVE SERVICE	Clicking this button removes the service from this bin. Unless addressed in a later bin, this service will automatically enter the lowest-priority bin listed.
BANDWIDTH	The allocated bandwidth given to the bin's services.
REMOVE BIN	Clicking this button removes this bin. Unless addressed in a later bin, the services the deleted bin contained will automatically enter the lowest-priority bin listed.
Add New Bin	Adds a new bin for service groupings.

9.5.1 Add Service

This section allows you to add a service into an existing bin.

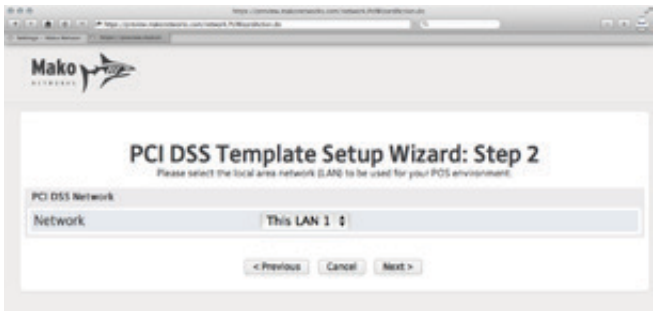
SERVICE	The contextual search field will filter results as you type. You may enter port numbers, service descriptions or substrings to find and select results. Service search This button is most useful for searching ranges of port addresses. It creates a pop-up form where you can enter a name or port to search with. Clicking on the resulting links enters the link into the **Service type** field.
BIN	Select the bin in which this service will be contained.
SOURCE IP	The Address from which data is for this service is active.

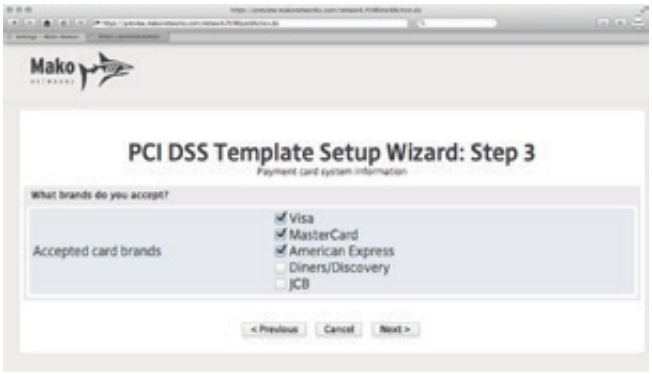
i Please ensure you have a large upstream capacity before exceeding 10 bins.


Welcome Jen Erick - last login: 25 August 2014 09:56 AM | History
Selected Mako: Example Company, Primary (DSL)
Configure
Services
PCI DSS
Settings
Home
Selection
Reports
Configure
Settings
No networks on the Mako appliance have had the PCI DSS Template applied. Begin the PCI DSS Wizard to apply the template to a network of your choice
PCI DSS Template Wizard

9.6 > PCI DSS


PCI DSS Template Setup Wizard: Step 1
Please read the terms and conditions. The checkbox below will be enabled once you have scrolled to the bottom.
Terms and Conditions
PCI DSS Template Wizard and optional QSA Bundle
I agree to the above terms and conditions
Cancel
Next >


PCI DSS Template Setup Wizard: Step 2
Please select the local area network (LAN) to be used for your POS environment.
PCI DSS Network
Network
This LAN 1
< Previous
Cancel
Next >


PCI DSS Template Setup Wizard: Step 3
Payment card system information
What brands do you accept?
Accepted card brands
Visa
MasterCard
American Express
Diners/Discovery
JCB
< Previous
Cancel
Next >


PCI DSS Template Setup Wizard: Step 4
Select your banking partner(s)
Bank Information
Bank
Select one
Add
Selected Banks
Bank
Delete
Westpac
ASB LTD
Choose your Payment Gateway(s)
Payment Gateway Information
Payment Gateway
Select one
Add
Selected Payment Gateways
Payment Gateway
Subnet
Delete
Elavon
62.17.112.113/255.255.255.255
195.245.90.61/255.255.255.255
193.155.119.61/255.255.255.255
194.36.113.137/255.255.255.255
213.168.228.13/255.255.255.255
Choose your QSA Provider
QSA Provider Information
QSA Provider
None
Add

9.6 > PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of rules set down by the PCI Security Standards Council that determine best practice for retailers who process credit card payments.

To activate the Mako PCI DSS service, you must first purchase a licence from your reseller. The Mako system is a certified PCI DSS Level 1 Networking and Security Service, which allows you to easily adopt the practice of PCI DSS compliance.

The Mako series features network segregation. The isolated network can be configured to run the compliant PCI DSS network on either LAN1 or LAN2; a non-compliant network can run on the other LAN port. The PCI DSS LAN is used for payment terminals.

Before beginning PCI DSS Activation, it's a good idea to get basic information about your network hardware ahead of time: printer and computer makes, models and serial numbers, related hardware IP Addresses

Activation

PCI DSS Template Wizard	This begins the 7-step process of making one of your Mako's LANs PCI DSS-compliant.

9.6.1 Step 1: Terms & Conditions

- Read the terms, and when ready, check "I agree to the above terms and conditions".

> Next

9.6.2 Step 2: LAN Selection

- Use the drop-down box to select the LAN to be designated PCI DSS compliant.

> Next

9.6.3 Step 3: Payment Card Brands

- Check the card brands this network accepts payments from.

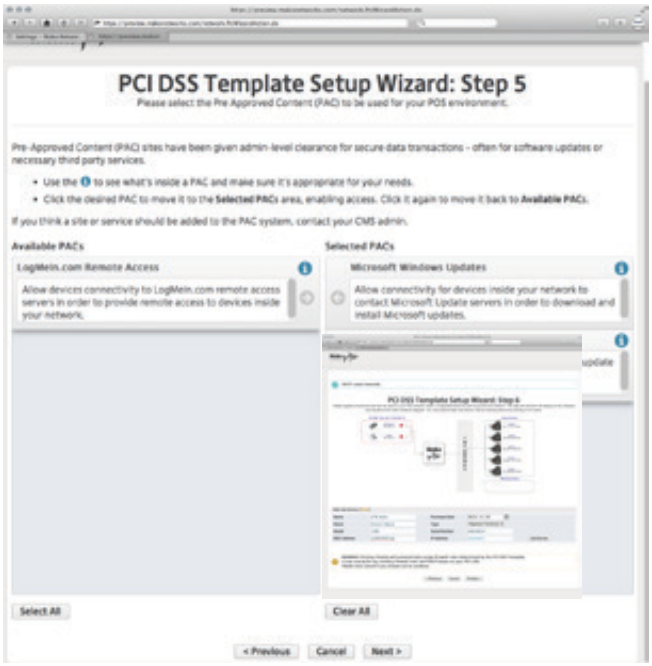
> Next

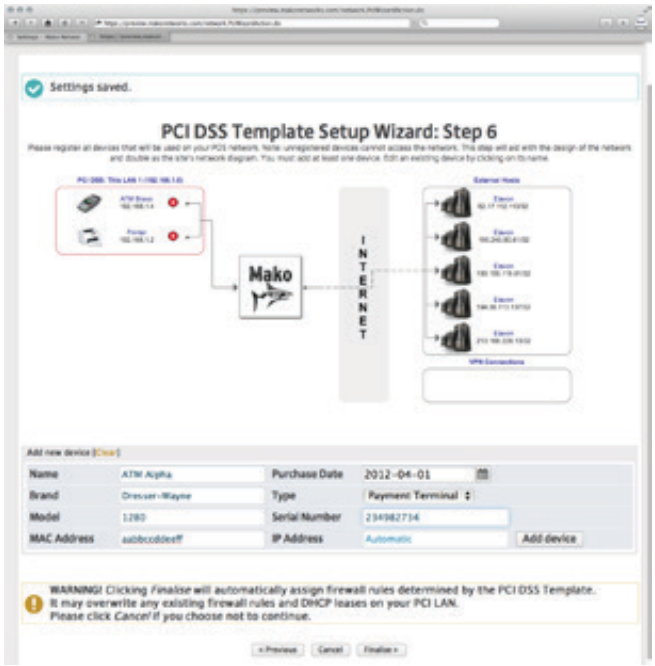
9.6.4 Step 4: Banks, Payment Gateways, Qualified Security Assessor

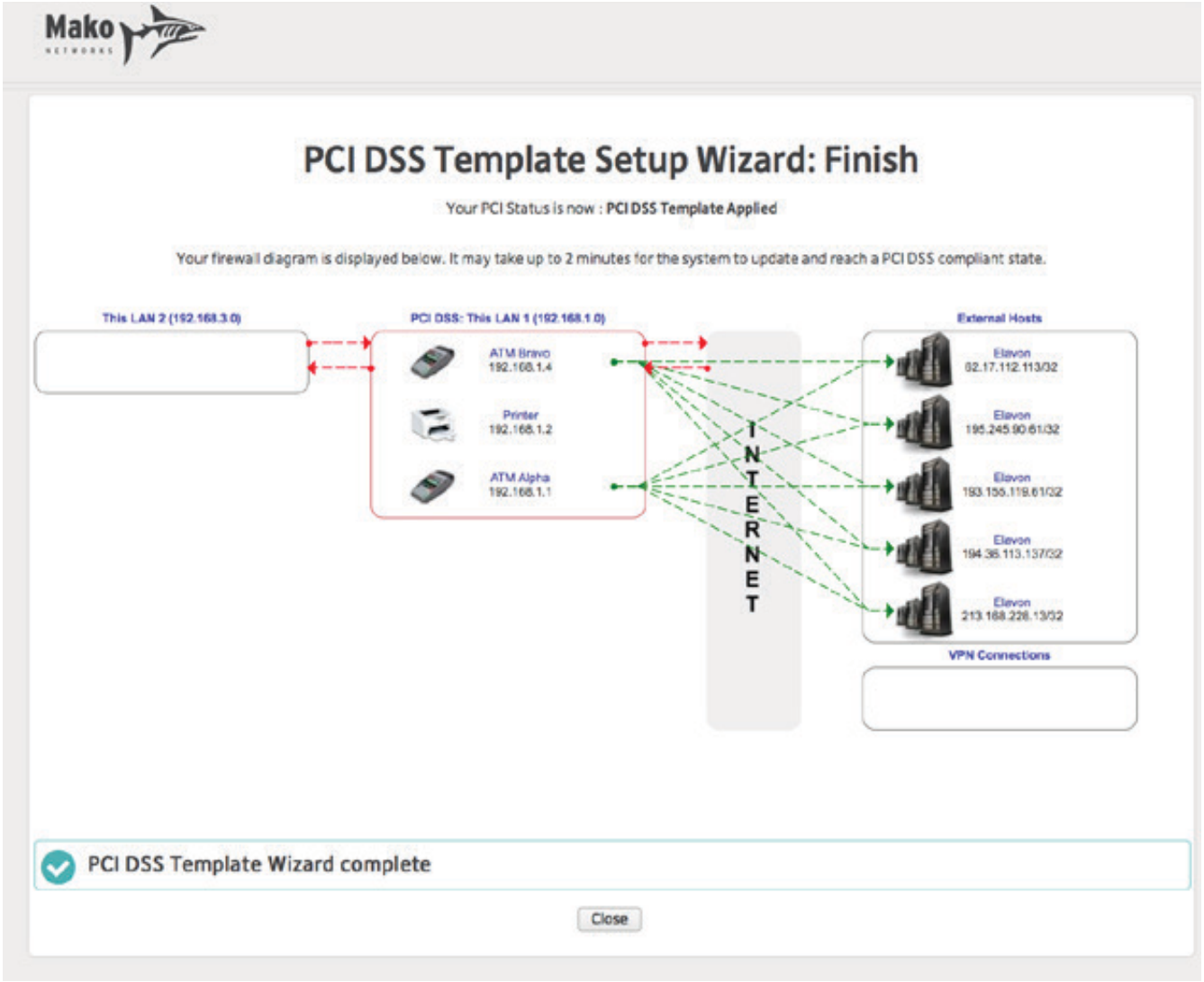
- Select a bank with which you process payments. Click **Add** after each bank you choose to add.
- Select a payment gateway with which you process payments. Click **Add** after each gateway you choose to add.
- Select your Qualified Security Assessor(s). Click **Add**. i

> Next

i Clicking Add in any section does not add the entire page's selections. Each detail must be added separately.


PCI DSS Template Setup Wizard: Step 5
Please select the Pre Approved Content (PAC) to be used for your POS environment.
Pre-Approved Content (PAC) sites have been given admin-level clearance for secure data transactions – often for software updates or necessary third party services.
Use the to see what's inside a PAC and make sure it's appropriate for your needs.
Click the desired PAC to move it to the Selected PACs area, enabling access. Click it again to move it back to Available PACs.
If you think a site or service should be added to the PAC system, contact your CMS admin.
Available PACs
Selected PACs
LogMein.com Remote Access
Allow devices connectivity to LogMein.com remote access servers in order to provide remote access to devices inside your network.
Microsoft Windows Updates
Allow connectivity for devices inside your network to contact Microsoft Update servers in order to download and install Microsoft updates.
Select All
Clear All
< Previous
Cancel
Next >


Settings saved.
PCI DSS Template Setup Wizard: Step 6
Mako
INTERNET
Add new device
Name
ATM Alpha
Purchase Date
2012-04-01
Brand
Dresser-Wayne
Type
Payment Terminal
Model
1280
Serial Number
234982734
MAC Address
aabbccddeeff
IP Address
Automatic
Add device
WARNING! Clicking Finalise will automatically assign firewall rules determined by the PCI DSS Template.
It may overwrite any existing firewall rules and DHCP leases on your PCI LAN.
Please click Cancel if you choose not to continue.


Mako
NETWORKS
PCI DSS Template Setup Wizard: Finish
Your PCI Status is now : PCI DSS Template Applied
Your firewall diagram is displayed below. It may take up to 2 minutes for the system to update and reach a PCI DSS compliant state.
This LAN 2 (192.168.3.0)
PCI DSS: This LAN 1 (192.168.1.0)
ATM Bravo
192.168.1.4
Printer
192.168.1.2
ATM Alpha
192.168.1.1
INTERNET
External Hosts
Elavon
62.17.112.113/32
Elavon
195.245.90.61/32
Elavon
193.155.119.61/32
Elavon
194.36.113.137/32
Elavon
213.168.226.13/32
VPN Connections
PCI DSS Template Wizard complete
Close

9.6.5 Step 5: Pre-Approved Content (PAC) Providers

The default condition after the PCI DSS template is applied is not to receive any traffic at all from external sources. However, critical/essential software services provided by third parties must remain available to get security updates and access. Pre-Approved Content (PAC) are common, legitimate, secure sources of essential services for operation.

- Click an arrow on an appropriate PAC to move it from 'Available' to 'Selected', or the reverse.
- Click ⓘ to inspect a PAC's contents. i

> Next

9.6.6 Step 6: Network Device Registration

PCI DSS Requirement 2.4 is the maintenance of an inventory system detailing the components of the PCI DSS network. Registering your hardware on this page creates that diagram for you.

The diagram itself is partially interactive: you may delete devices with a corresponding x button, or hover over a device to obtain its details. Clicking on a local device's icon title ('Printer', 'ATM', etc.) will populate the lower Add Device section, to modify its details.

Add New Device

NAME	A meaningful name for the device.
BRAND	The device brand.
MODEL	The device model.
MAC ADDRESS	The device MAC Address.
PURCHASE DATE	The date when it was purchased.
TYPE	Payment Terminal / Printer / Computer / Storage: select the kind of device it is.
SERIAL NUMBER	The device serial number. This could be printed on the device or recalled electronically.
IP ADDRESS	The IP Address for this device. You may wish to leave this unassigned and let the Mako assign the address dynamically.

> Finalise

9.6.7 Network Summary

Your network diagram is produced.

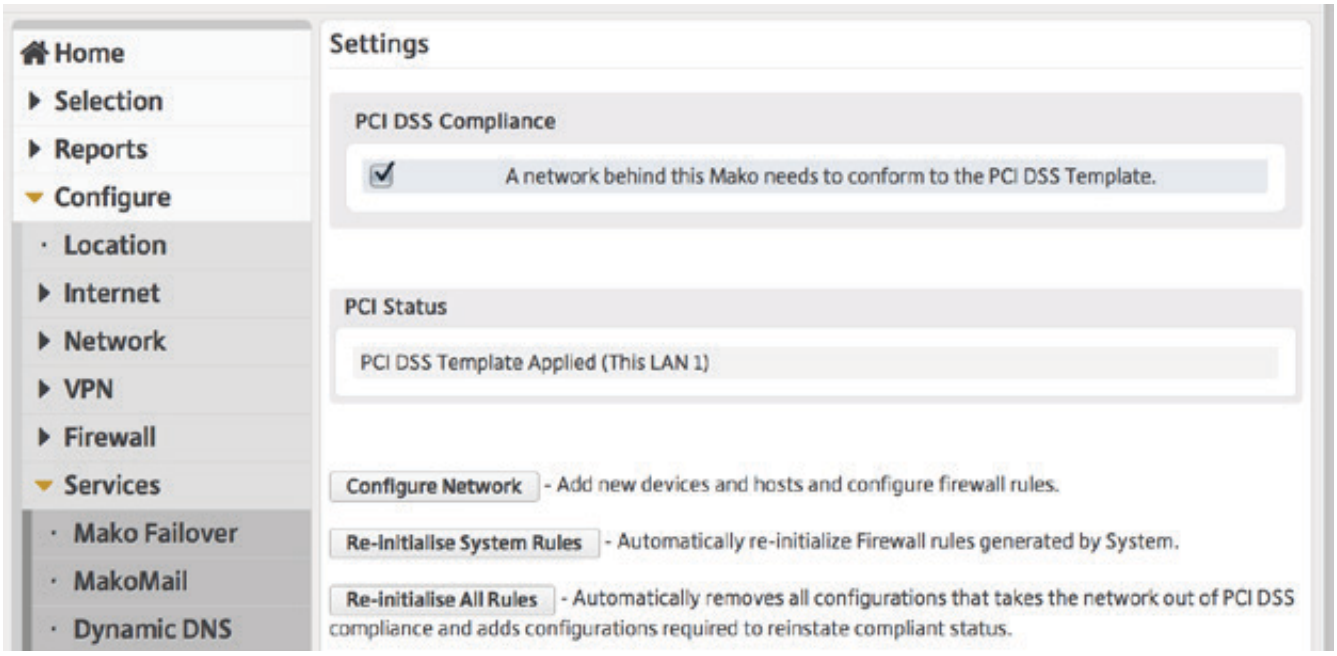
Red arrows indicate traffic flow is physically possible, but has been disabled.

Green arrows indicate permitted firewall-allowed/pinhole-allowed routes, and direction of flow.

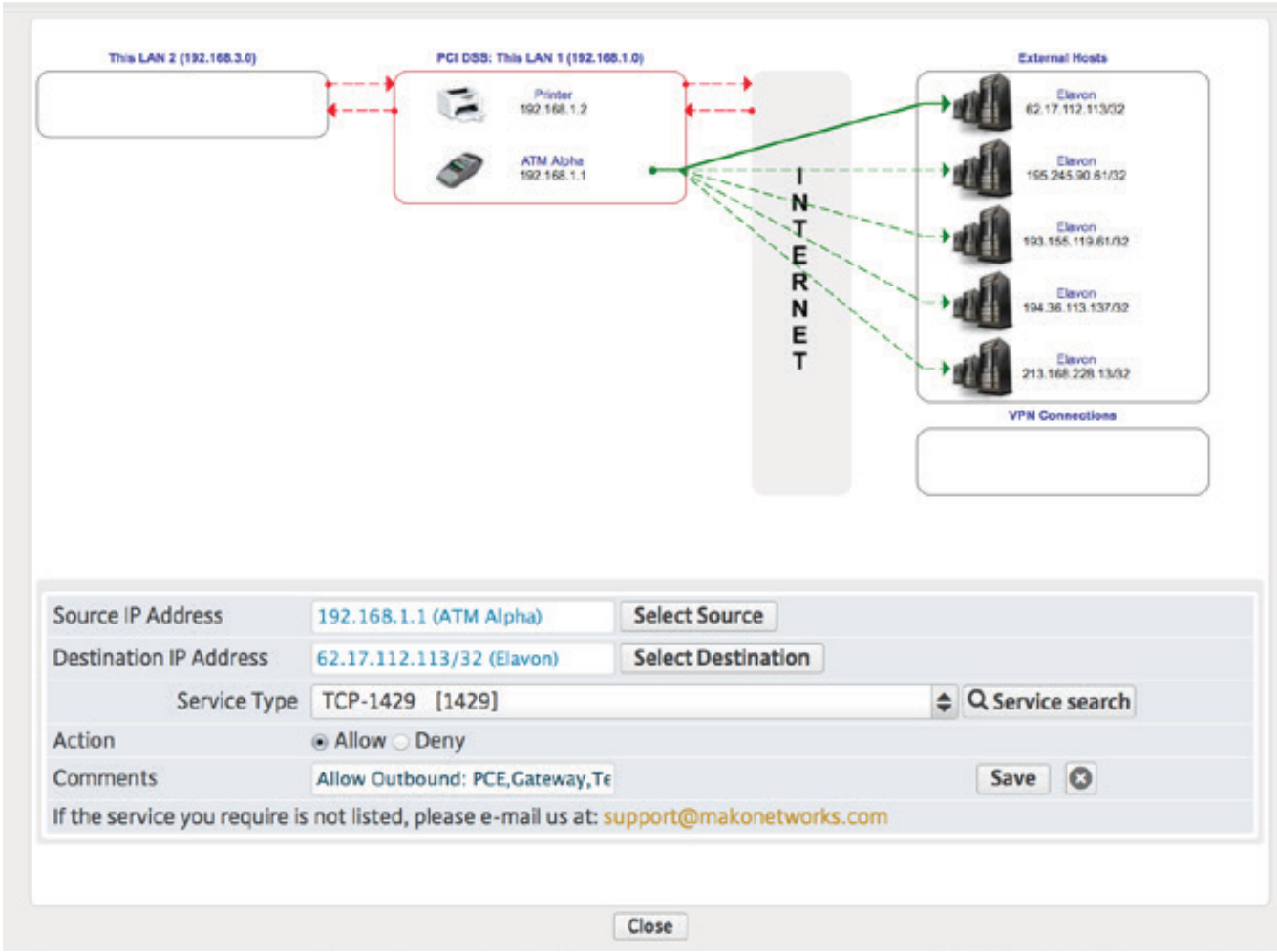
The PCI Template is complete, and PCI DSS compliance is in force for the selected LAN.

---

i If you think a site or service should be added to the PAC system, contact your CMS admin.



9.8 CHANGING THE PCI DSS TEMPLATE



9.8.2 ADDITIONAL PCI DSS FUNCTIONS: HARDWARE CHANGES, RE-APPLYING THE PCI DSS TEMPLATE

9.7 › New PCI DSS Pages

When the PCI DSS Template has been applied to the LAN, individual pages appear in the main menu for the sections used in the PCI DSS Template Wizard: **Settings**, **Banks**, **Gateways**, **QSA Bundle** and **PAC Selection**.

9.8 Changing the PCI DSS Template

PCI DSS Compliance is an on-going, business-specific process.

Some (not any, or all) changes may be made to modify the PCI DSS Template, provided you document the changes and provide business justifications in a compliant manner. **But if the PCI Template is modified then your network is outside the scope of the Mako System's ability to enforce PCI Compliance.**

9.8.1 Altering PCI DSS Template LAN Configurations

Changing settings that change the PCI DSS Template will require both a re-entry of your user password and a business justification. The change will be logged and transmitted to your bank/payment gateway.

9.8.2 Additional PCI DSS Functions: Hardware changes, Re-applying the PCI DSS Template

Once the PCI DSS Template has been enabled you may add/delete hardware, reset Mako System firewall rules to the template, or set all rules to the template.

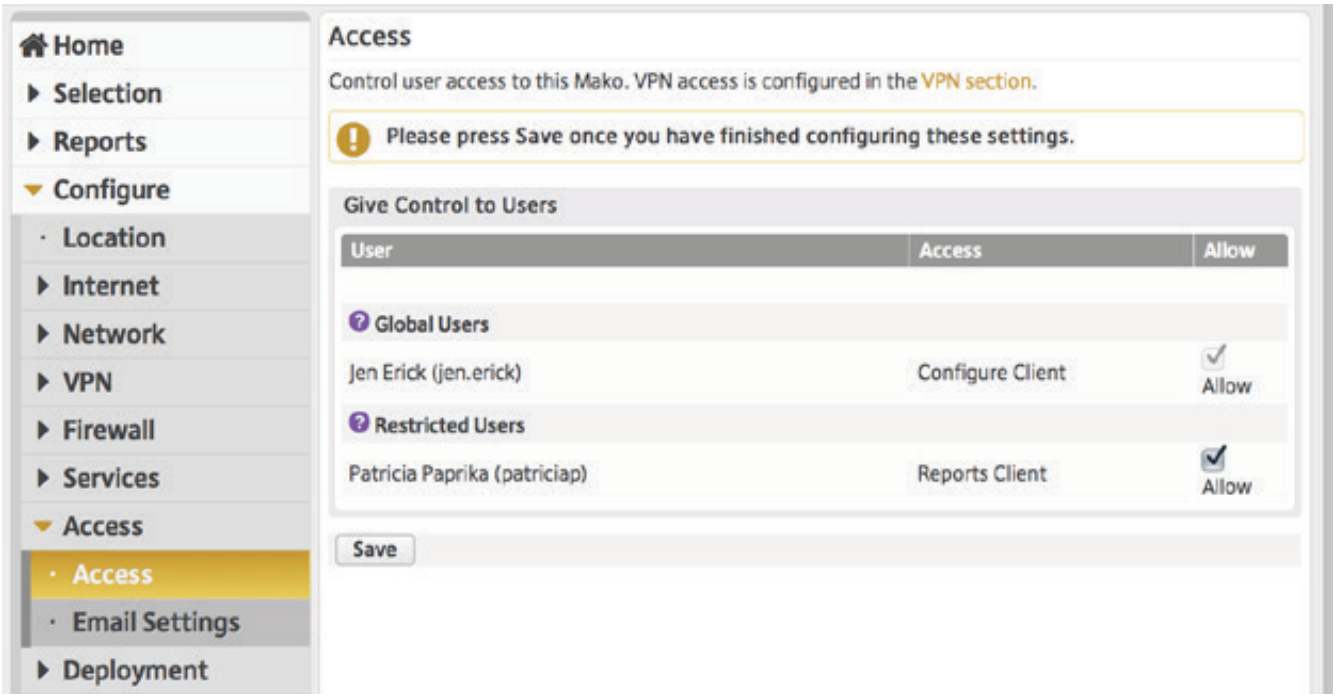
- Configure > Service > PCI DSS > Settings

CONFIGURE NETWORK	Takes you to the network diagram page, where you can: : Delete a device from the LAN **Add new device**: Enter the details of the new device. Firewall Rules: Each green arrow represents a firewall rule between two devices. Clicking on an arrow loads the firewall rule details, which you can inspect or alter.
RE-INITIALISE SYSTEM RULES	This button automatically re-applies the PCI DSS Template rules generated by the Mako System.
RE-INITIALISE ALL RULES	This button automatically removes all configurations that takes the network out of PCI DSS compliance and adds configurations required to reinstate compliant status.

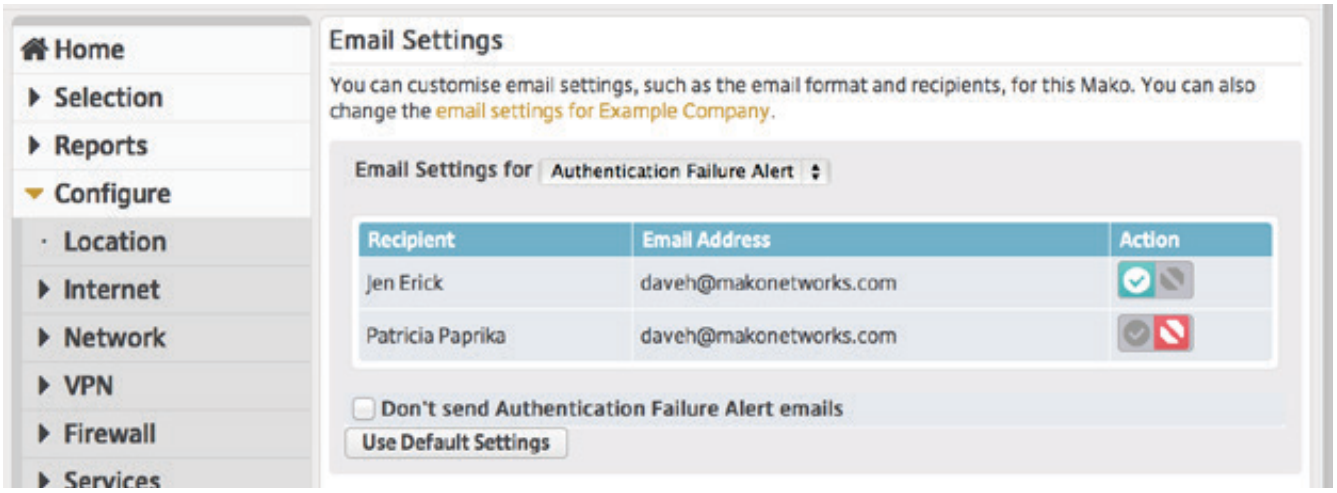
9.9 › Mako Guardian

Mako Guardian is an active web content filtering and laundering service that gives you total control over the web content that is allowed into your network. With Mako Guardian you can meet legal requirements to control access to objectionable or inappropriate websites.

To activate Mako Guardian, you must first purchase a licence from your reseller. Refer to the Mako Guardian manual for details on using this add on.



10.1 > ACCESS



10.2 > EMAIL SETTINGS

10 Configure > Access

10.1 > Access

The Access page displays a list of users that have VPN access to this Mako.

- Check the names in the appropriate sections to give these users access to your network. [i]

Save when finished.

10.2 > Email Settings

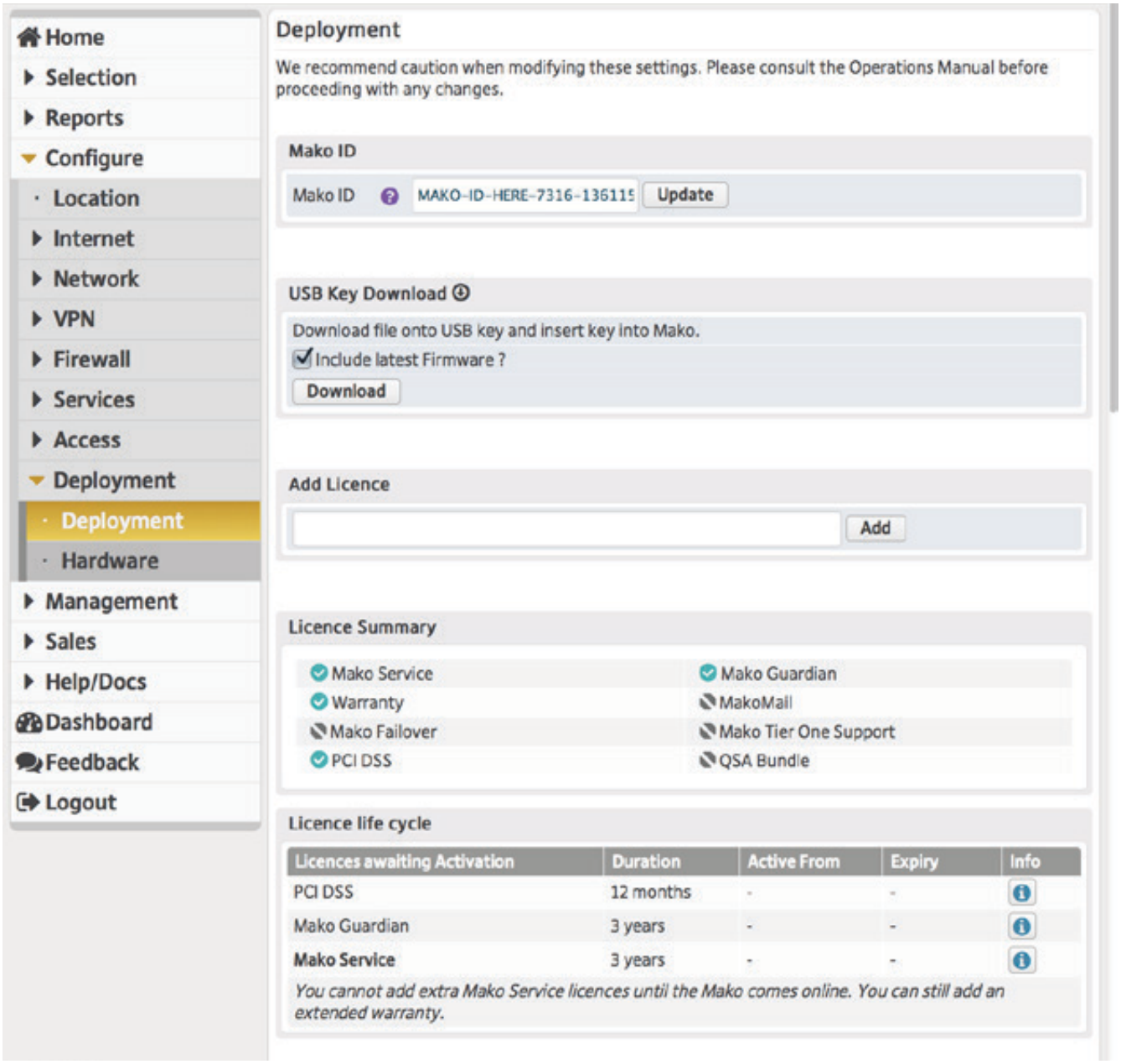
The Email Settings page lets you choose which users receive important email reports from the Mako System.

- Select your report type in the drop-down menu.
- Click on the or icon to allow or deny this report respectively.
- Repeat this process for the relevant reports presented in the drop-down menu. [ii]
- **Don't send *[report name]* emails**: Check this box if no users are to receive the selected report.
- The link "email settings for Example Company" takes you to Management > Manage [Company Name] > Custom Settings > *Email Settings...*

---

[i] At least two users must be assigned to a Mako before any user options will appear, and you must have administrative rights in order to change a user's permissions.

[ii] There is no Save button on this page, as your input is saved when you change an Action state for a user.



11.1 > DEPLOYMENT

11 Configure > Deployment

11.1 > Deployment

Deployment is the process of installing your Mako for the first time and getting it connected to the CMS. Often 'deployment' refers to activating a number of Makos at the same time.

MAKO ID

This is the 12-character MAC address located at the back of a 6500-Series Mako, or under a top-level menu within the 7500 and 8000-Series concentrators.

USB KEY DOWNLOAD

When a Mako connects to the Internet for the first time, it's pre-programmed to contact the CMS and download the latest configuration files. But for 'push play' operation on large deployments this may be impractical, or you may not have a stable Internet connection for the Mako when you deploy it.

This function downloads the file 'configuration.zip' to a computer so you can pre-configure it. Copy this file to a FAT–32 formatted USB stick, insert the stick into the Mako, and connect the Mako to power.

Include latest Firmware?

Download

This option incorporates additional configuration files into 'configuration.zip'.

Do not expand 'configuration.zip' before inserting the stick into your Mako - The Mako is geared to receive a specific filename with the .zip format, for a specific USB format.

ADD LICENSE

When given a license to use an optional service you will be sent a license code. Enter this code here.

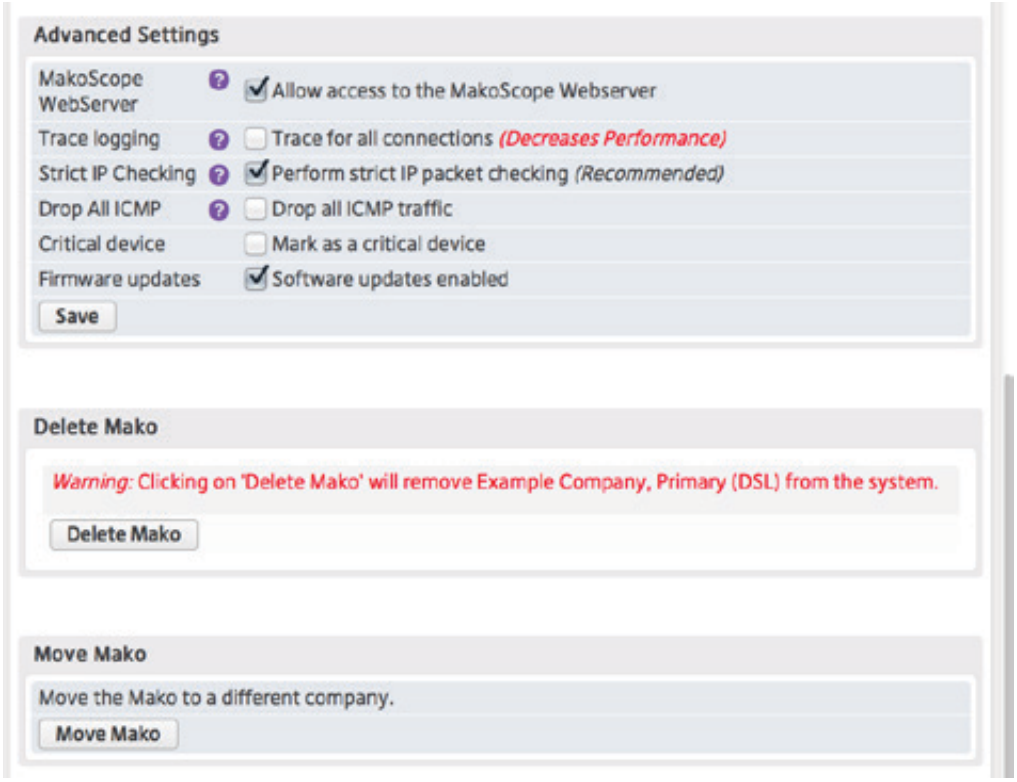
LICENSE SUMMARY

A list of all licenses and their statuses.

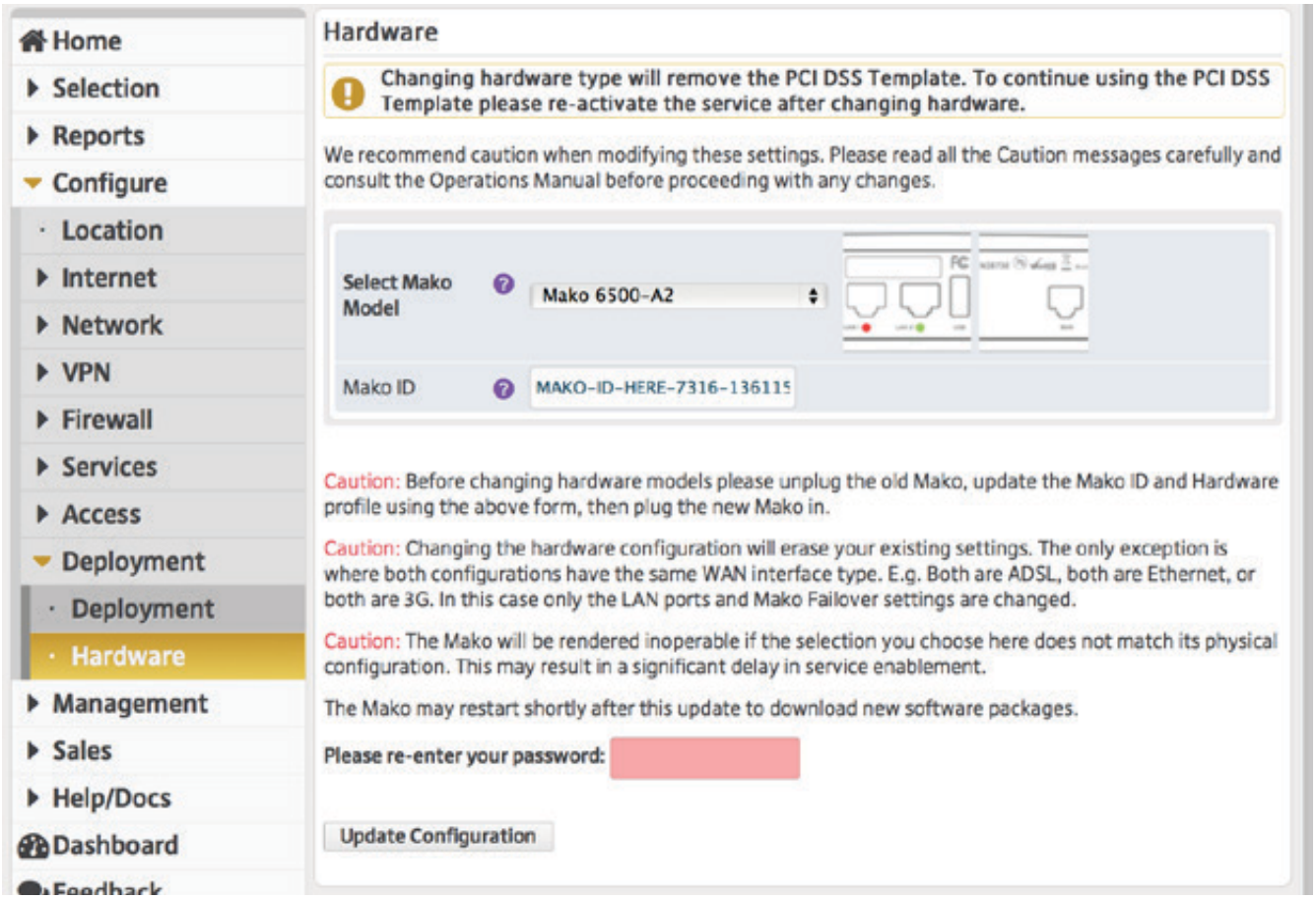
Note: Mako Failover no longer requires a license and comes standard between all Makos of the same series number (6500 series, 7000 series, 8000 series)

LICENSE LIFE CYCLE

This form breaks down what each service license offers. The ⓘ button provides additional details for that license.



11.1 > DEPLOYMENT - ADVANCED SETTINGS



11.2 > HARDWARE

ADVANCED SETTINGS

Makoscope Webserver: This 'master switch is currently disabled, as it's present for each LAN under Configure > LAN 1 ... LAN x.

Trace Logging: This 'master switch' is currently disabled. Specific trace logging of IPs and firewalls are present for each firewall rule under Configure > Firewall > Inbound/Outbound/Intranet/VPN > Advanced.

Strict IP Checking: Checking this box ensures all IP packets passing through the firewall are not malformed or invalid. Unchecked, some checks are still performed but not all. (Some applications are known to work only if Strict IP Checking is enabled.)

Drop All ICMP: Checking this box ensures all ICMP traffic is blocked. Blocking ICMP traffic is used to prevent ICMP replay attacks, however this will make tools such as ping and traceroute inoperable.

Critical Device: Marking the selected device as a critical device means several settings will require password authentication. This is often applied to concentrators to prevent accidental misconfigurations.

DELETE MAKO

Delete Mako

Pressing this button takes you to an authentication step where you can Cancel or Delete the currently selected Mako. Pressing this button also 'unhides' this menu option from the Configure > Deployment section.

MOVE MAKO

Move Mako

Pressing this button takes you to an authentication step where you can Cancel or Delete the currently selected Mako. Pressing this button also 'unhides' this menu option from the main menu.

11.2 › Hardware

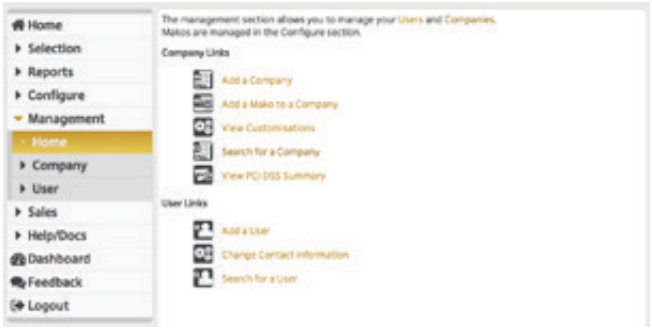
This section allows you to re-assign a different Mako Model to the Mako currently selected. This is usually used to swap out defective hardware.

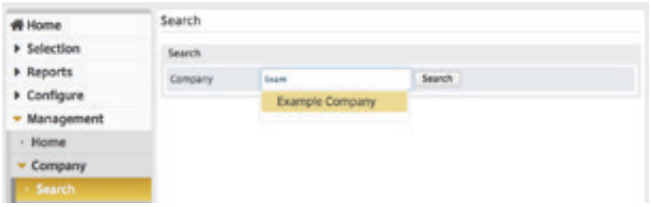
Several considerations need to be addressed for this operation. Please use the following sequence.

- Note the incoming Mako's MakoID.
- **Unless both configurations have the same WAN interface type, changing the hardware configuration will erase your existing settings.** So to ensure settings are carried over, both the outgoing and incoming Makos must be both Ethernet Makos, or both DSL Makos.
- Note: the Mako 6500-M and M/LTE may use Ethernet, DSL, LTE or dial-up for a WAN, but settings will still be lost if you attempt to change out a Mako 6500-A2, for instance, for a 6500-M.
- Disconnect the outgoing Mako.
- Enter the incoming Mako's MakoID.
- Select the incoming Mako's hardware profile from the drop-down menu.
- Connect the incoming Mako to power and WAN.

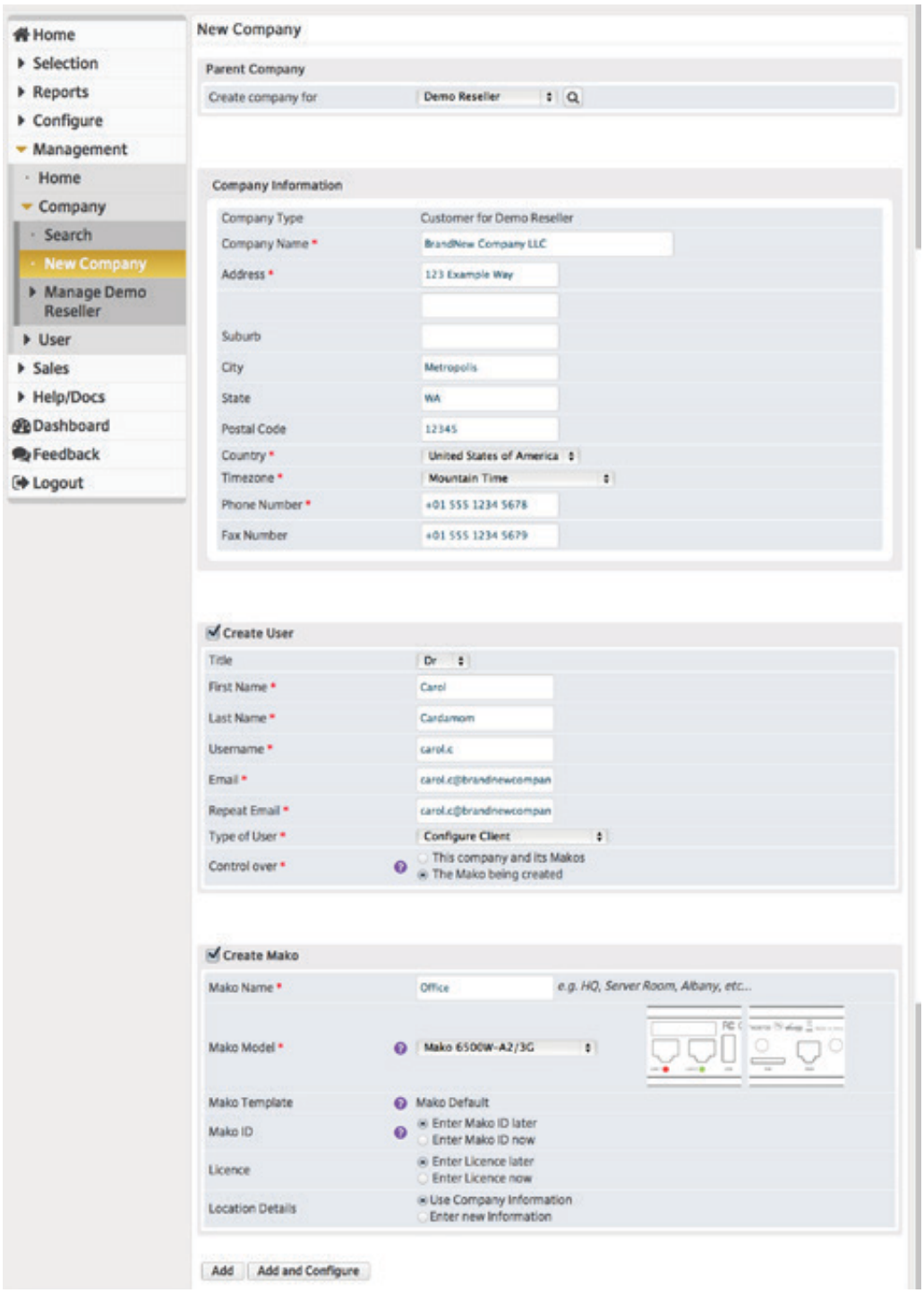
The Mako will be rendered inoperable if the selected hardware profile doesn't match the incoming Mako's. This may result in a significant delay in the start of service.

The Mako may restart shortly after this update to download new software packages.





12.3 > NEW COMPANY



12 Management > Company

The management section focuses on managing pre-existing or pre-configured Makos, users, companies, VPNs and systems, rather than setting up systems. Once set, your network administrators will manage the network through these pages. [i]

12.1 > Home

The Management section is for administering User and Company information. By default, your own User and Company are selected and shown in the header section.

This section's landing page contains links to related and regularly-accessed parts of the CMS.

12.2 > Search

- Enter a Company name here to list the Makos you can administer.

Search when finished.

12.3 > New Company

If you have appropriate access, this page provides all necessary fields for creating a company and at least one Mako you can assign to it.

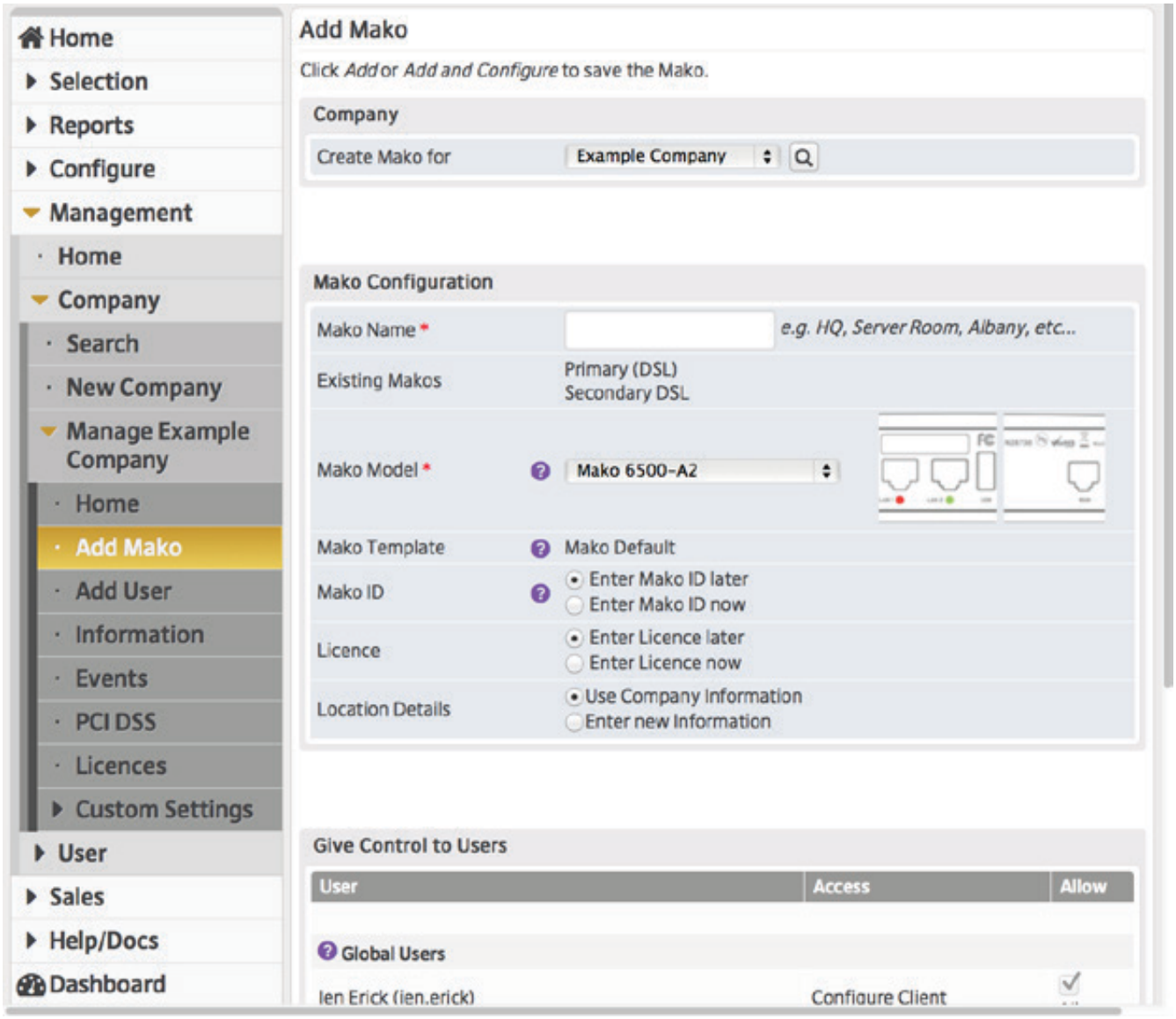
- Go through the page and fill in the necessary details. [ii]
- Descriptions of the fields in the Add Mako form may be found here: *> Add Mako...*

Add, or Add and Configure when finished.

---

[i] When you enter the Management section, the Header bar information will change to reflect company information rather than Mako-specific information.

[ii] All asterisked fields are necessary for company creation.



12.4.2 > ADD MAKO

12.4 › Manage [Company name]

This section gives you company-specific access to functions already covered in the Configure section.

12.4.1 › Home

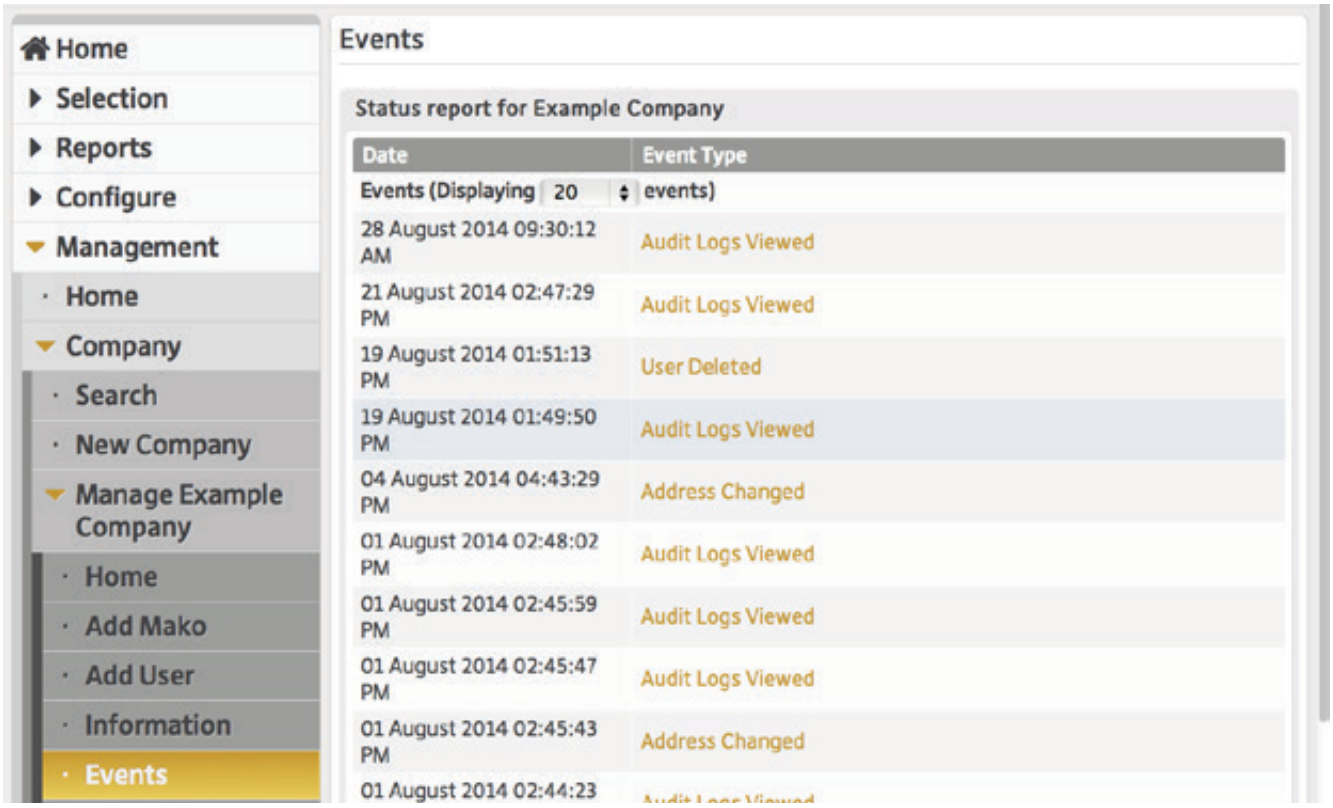
This section's landing page contains links to related and regularly-accessed parts of the CMS.

12.4.2 › Add Mako

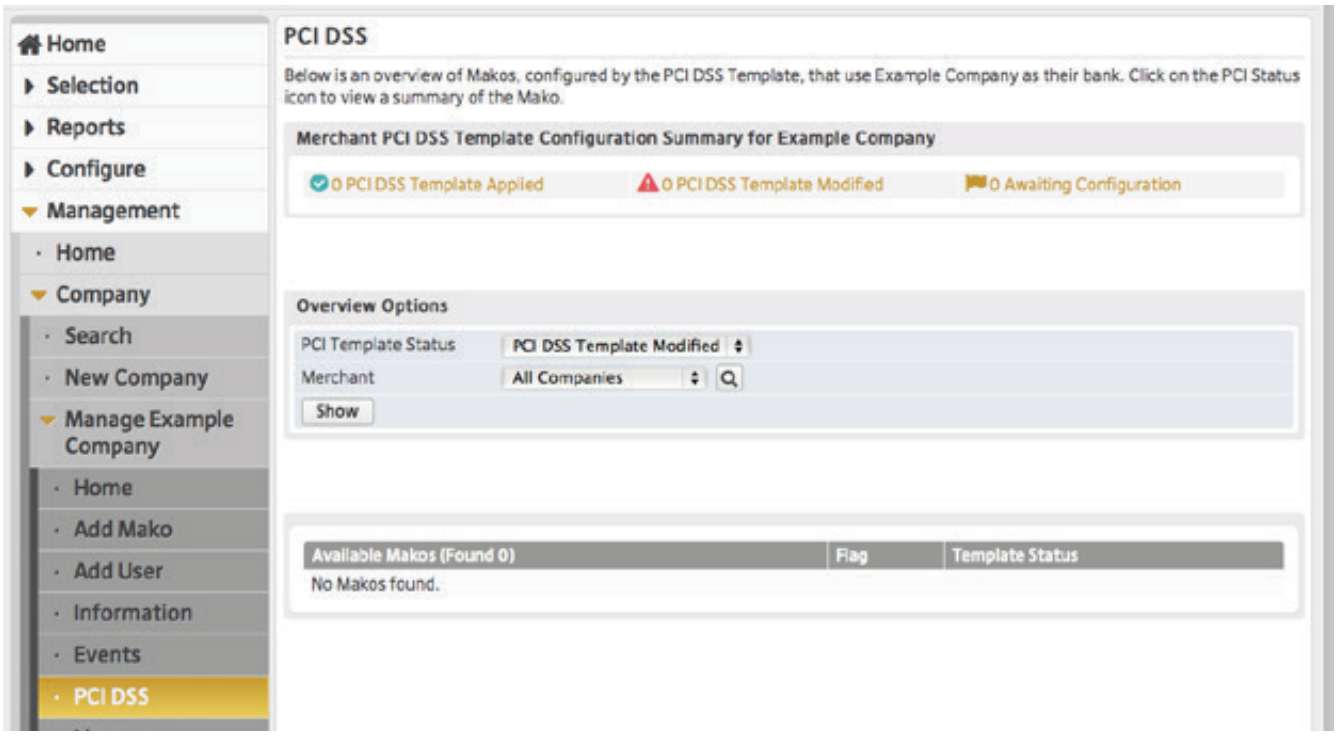
If you have appropriate access, this page allows you to add a new Mako to a selected company's network.

COMPANY	A list of companies to which you have **Add Mako** permissions.
MAKO NAME	A unique, useful name for the Mako to be added.
EXISTING MAKOS	A list of Makos within the company's network, serving as a guide to how this network names its Makos.
MAKO MODEL	Select the Mako model for this Mako. This must be exact. You may find the Mako Model printed on the back of a 6500. 7550 concentrators come in a 'Lite', 2-LAN enabled version, or a standard 4-LAN enabled device, but are identical. If you're not sure which device you're loading, ask your reseller.
MAKO TEMPLATE	The template contains security presets such as firewall configurations.
MAKOID	The 12-character ID for this Mako. Found on the back of 6500 models or within the menu of the Mako concentrators.
LICENSE	Licenses are required for value-added features within the Mako System. You may purchase them by contacting your reseller.
LOCATION DETAILS	Physical location details for this Mako. You may enter new details, or copy the default company details to this Mako.
GIVE CONTROL TO USERS	Registered, access-permitted users may be given control of this Mako by checking the user's associated 'Allow' box.

- Click **Add** or **Add and Configure** when finished.



12.4.5 > EVENTS



12.4.6 > PCI DSS

12.4.3 › Add User

If you have appropriate access, you may add a new user to the company's network.

Enter the company information into the appropriate fields. All user information fields are mandatory.

- Click **Add** when finished.

12.4.4 › Information

This contains a summary of company information, including parent relations: the companies or service providers that govern this network or company. If you have appropriate access you may delete this company from this page, or edit details.

12.4.5 › Events

This lists the recent changes to the company records of this company, such as physical address changes, user additions or if this Event log was viewed. Linked events display more detail about the log.

12.4.6 › PCI DSS

This is an overview of Makos configured by the PCI DSS Template, that use the selected company as their bank.

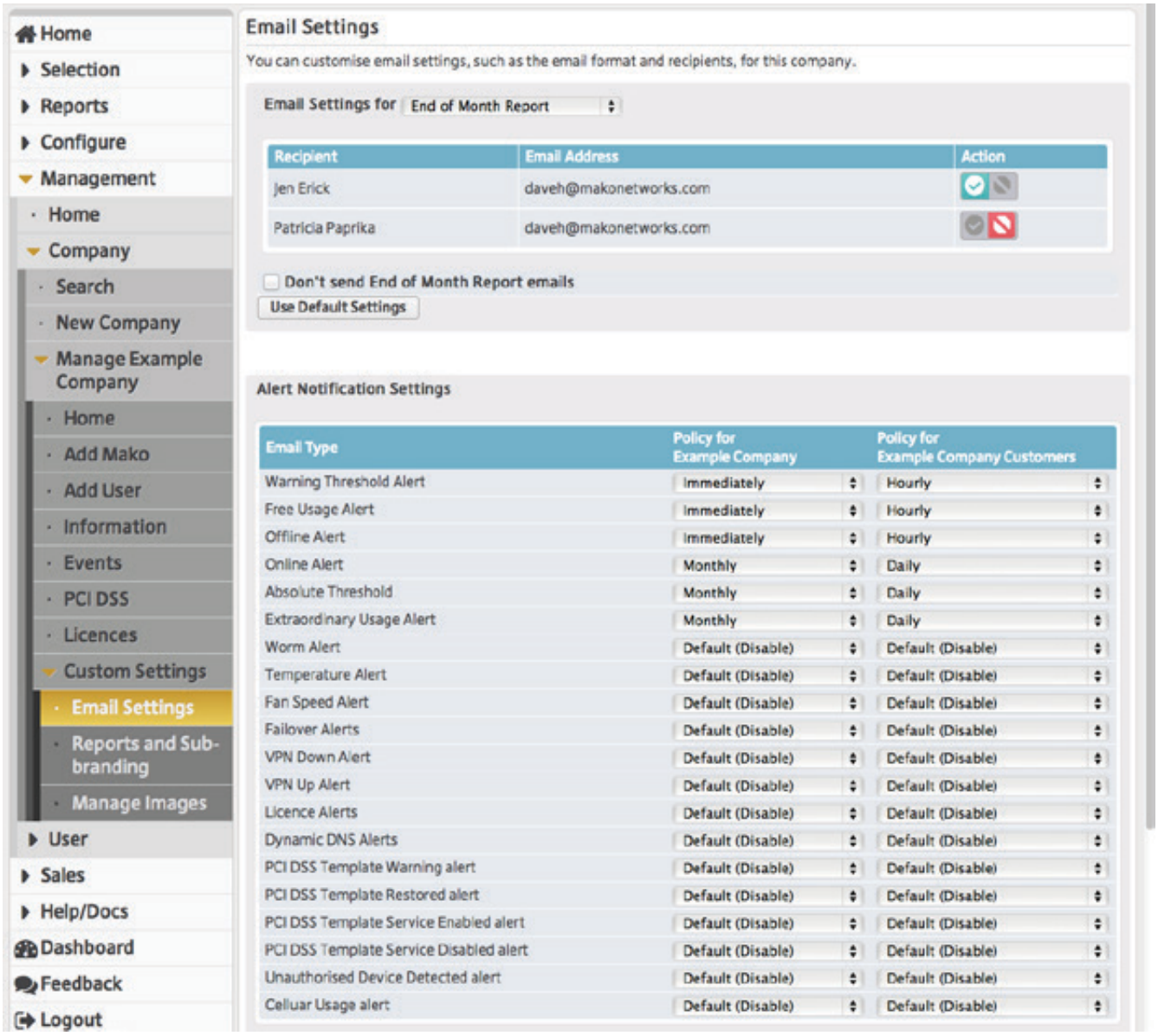
- Select the **PCI Template Status** type and **Merchant**.
- Click **Show** when finished.

12.4.7 › Licences

Resellers and high-level administrators create time-based permissions for users of a Mako system. This gives your system an ability to maintain current security checks.

This page creates reports for the Company or users under the company's Mako system.

- Select the **company**, **scope** and **format** for your report.
- If required, check **Ignore temporary initial licenses**.
- **Search** when finished.



12.5.2 > EMAIL SETTINGS: ALERT NOTIFICATION SETTINGS

12.5 › Custom Settings

12.5.1 › Email Settings

Email Settings affects which reports are sent to subscribing users, and how often. The top section deals with general reports and who should receive them. The lower section deals with Alerts, and allows you to prioritize and schedule them as you wish.

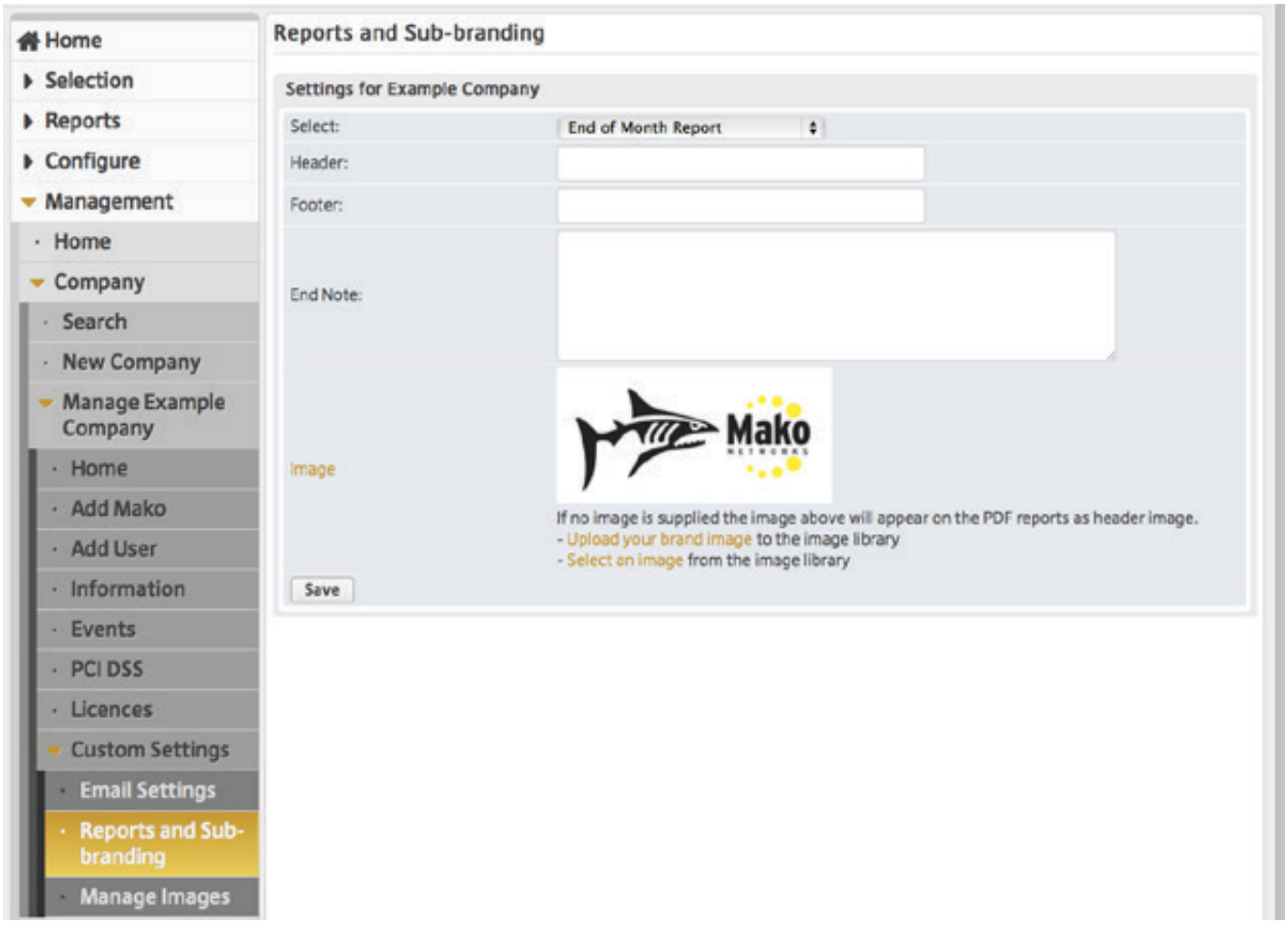
EMAIL SETTINGS FOR [REPORT]	Select the report type.
ACTION	Set the Allow or Deny permission here.
DON'T SEND [REPORT NAME] EMAILS	This disables the report being sent to all users.
Use Default Settings	This button affects BOTH sections of this page. If an admin has created defaults for both reports and alerts, this will reset all values to those defaults.

12.5.2 › Email Settings: Alert Notification Settings

Each Email type may be scheduled for an appropriate send-time, or have it disabled. Scheduling policy applies to two audiences: Those users of the selected company, and those users who are customers/ subsidiary networks of the selected company.

Settings are: **Default**, **Immediately**, **Hourly**, **Daily**, **Weekly**, **Monthly** or **Disable**. The Default value is assigned by a company admin.

- **Save** when finished.



12.5.3 > REPORTS AND SUB-BRANDING

12.5.3 › Reports and Sub-branding

This page allows you to customize the look of 4 reports: **Company-wide Summary**, **End of Month**, **Sharknet IDS Report** and **PCI DSS Information**.

Select the report you wish to customize. You'll be presented with **Header**, **Footer**, **End Note** and an **image**-select fields.

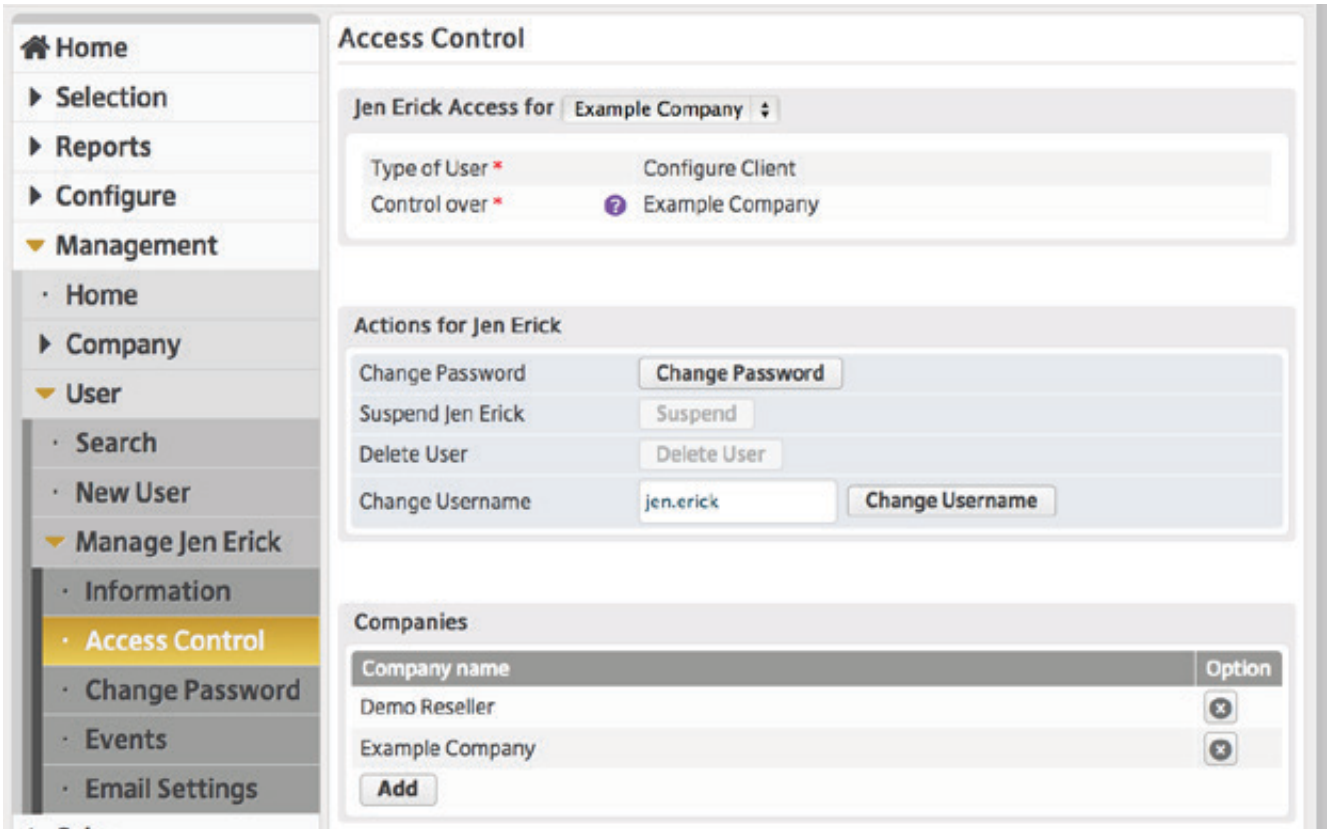
- Enter appropriate information in the fields.
- Press **Load** or the Image link to take you to the **Manage Images** page.

Save when finished.

12.6 › Manage Images

This page allows you to load logos for report and branding uses throughout the site.

- Click the **Browse...** button and navigate your way to your locally-stored logo.
- **Upload Logo** when finished.



13.3 > MANAGE [USER NAME]

13 Management > User

13.1 > Search

The User section collates features similar to company-specific features detailed earlier.

- Select a Company name here to list the users you can administer. The button allows you to enter free text, if you have a very long list of customers. Clicking the 🔍 icon will allow you to enter a Company name within which to search for users.
- **Search** when finished. A list of users under that company will appear.

13.2 > New User

This page allows you to add new users to this company.

(To add VPN users: **Configure > VPN** *> Remote Access > Add VPN User...*)

- Go through the page and fill in the necessary details.
- **Type of User**: These user types define what type of access the user will have to the Mako System.
- **Control over**: This setting defines the scope of access this user will have to the selected company and its Makos. If selecting "One or more Makos for [Company]", an additional pop-up will appear where you may individually select Makos for the new user to access.
- **Add** when finished.

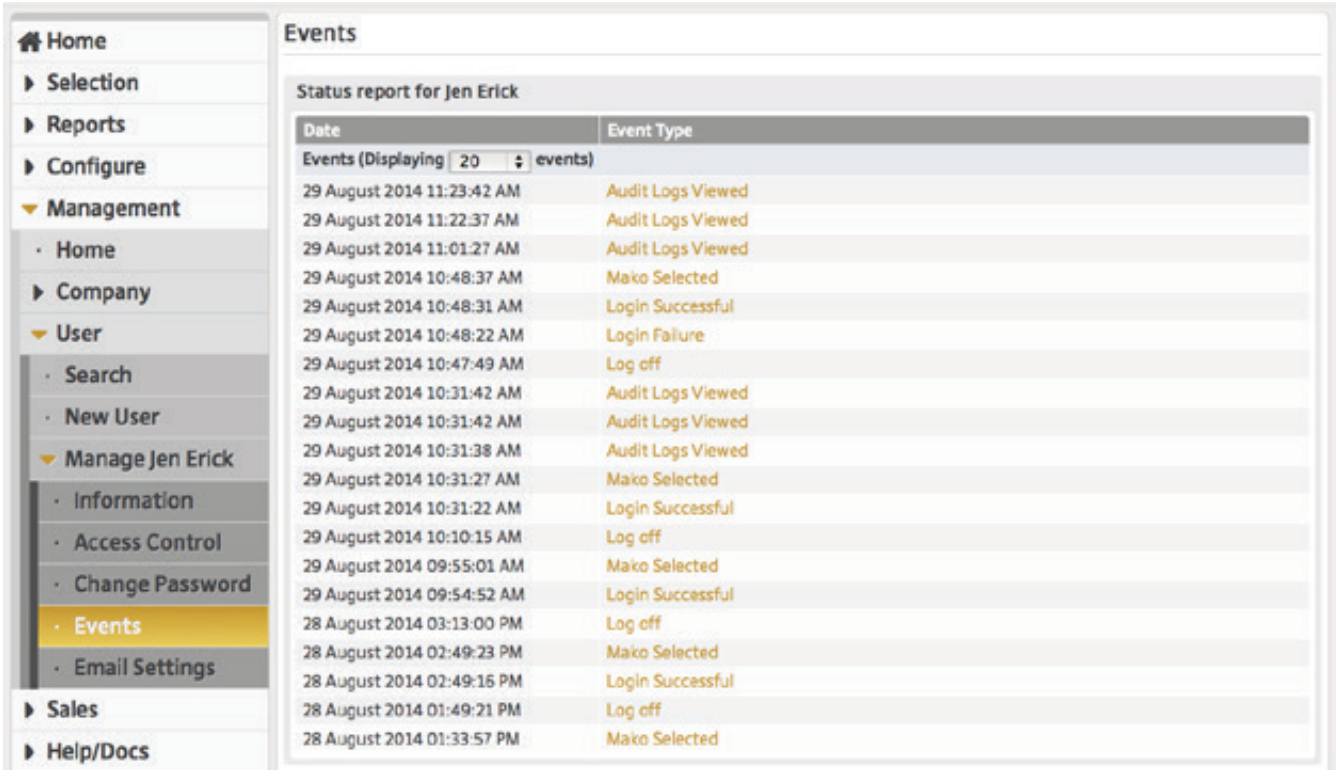
13.3 > Manage [User Name]

This sub-section collates the current user's information to create user-specific preferences.

13.3.1 > Information

A summary of physical/contact info for the select user. Edit allows you to edit details of the user. Access Control links you to the next section.

ACCESS CONTROL	Password and governance controls over the user. You cannot change your own Access level, only the Users you have created. You may only grant other users access equal to or less than your own access.
CHANGE PASSWORD	Takes you to the **Change Password** page.
SUSPEND [NAME]	This effectively deactivates the account, but doesn't delete its information. This button maybe disabled if you are logged in as this user, or not visible at all if you don't have permissions for this action.
DELETE USER:	Remove the user from the system. This button maybe disabled if you are logged in as this user, or not visible at all if you don't have permissions for this action.
CHANGE USERNAME:	Enter a new username. **Change Username** when finished.


Home
Selection
Reports
Configure
Management
Home
Company
User
Search
New User
Manage Jen Erick
Information
Access Control
Change Password
Events
Email Settings
Sales
Help/Docs
Events
Status report for Jen Erick
Date
Event Type
Events (Displaying 20 events)
29 August 2014 11:23:42 AM Audit Logs Viewed
29 August 2014 11:22:37 AM Audit Logs Viewed
29 August 2014 11:01:27 AM Audit Logs Viewed
29 August 2014 10:48:37 AM Mako Selected
29 August 2014 10:48:31 AM Login Successful
29 August 2014 10:48:22 AM Login Failure
29 August 2014 10:47:49 AM Log off
29 August 2014 10:31:42 AM Audit Logs Viewed
29 August 2014 10:31:42 AM Audit Logs Viewed
29 August 2014 10:31:38 AM Audit Logs Viewed
29 August 2014 10:31:27 AM Mako Selected
29 August 2014 10:31:22 AM Login Successful
29 August 2014 10:10:15 AM Log off
29 August 2014 09:55:01 AM Mako Selected
29 August 2014 09:54:52 AM Login Successful
28 August 2014 03:13:00 PM Log off
28 August 2014 02:49:23 PM Mako Selected
28 August 2014 02:49:16 PM Login Successful
28 August 2014 01:49:21 PM Log off
28 August 2014 01:33:57 PM Mako Selected

13.4 > EVENTS

13.3.2 Companies

This lists the companies to which the user account is affiliated.

Add	This button leads to a search field to find a new company the selected user may access.
OPTION	deletes access to this company for the selected user.

13.4 > Events

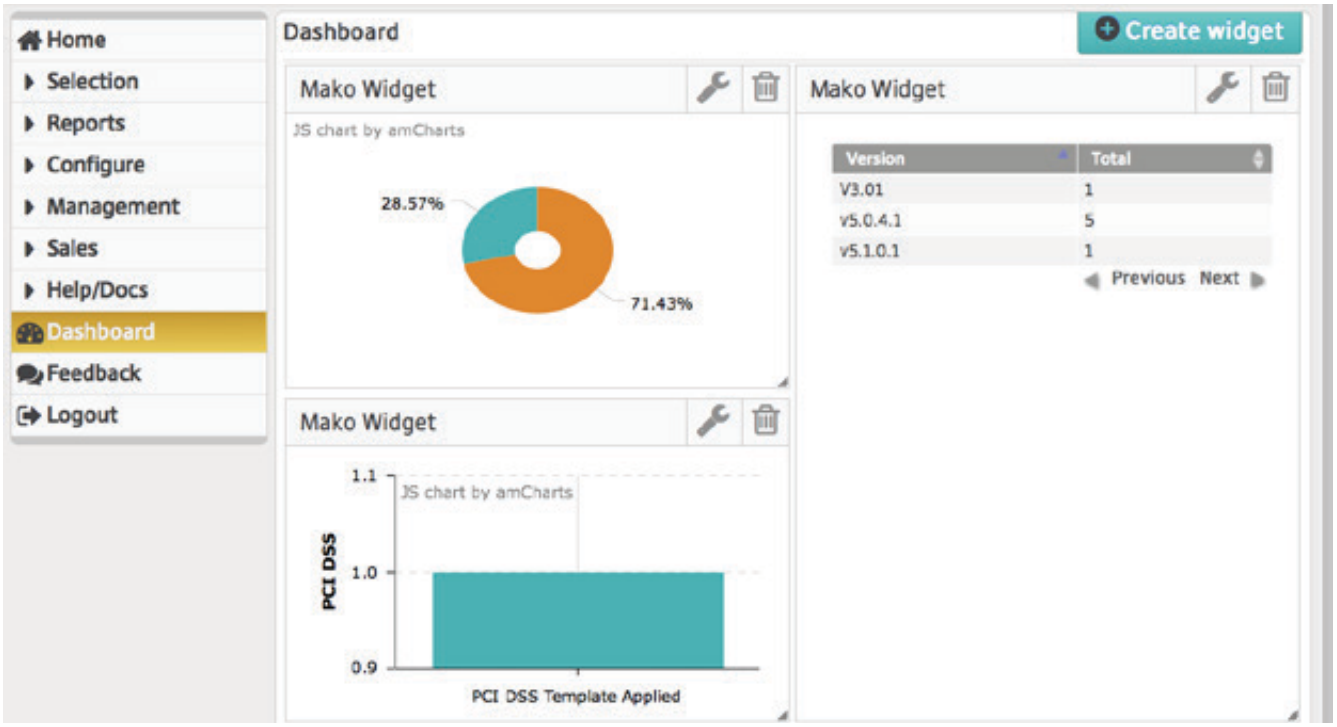
A log of changes that have been made to your Company is available here.

- Set the number of events you wish to display, and click the links for log specifics.

13.5 > Email Settings

Like the company-wide page Management > Company > Manage [Name] >Custom Settings > *Email Settings...* This sets notification policies, but for personal tailoring. i

i These settings override company defaults.

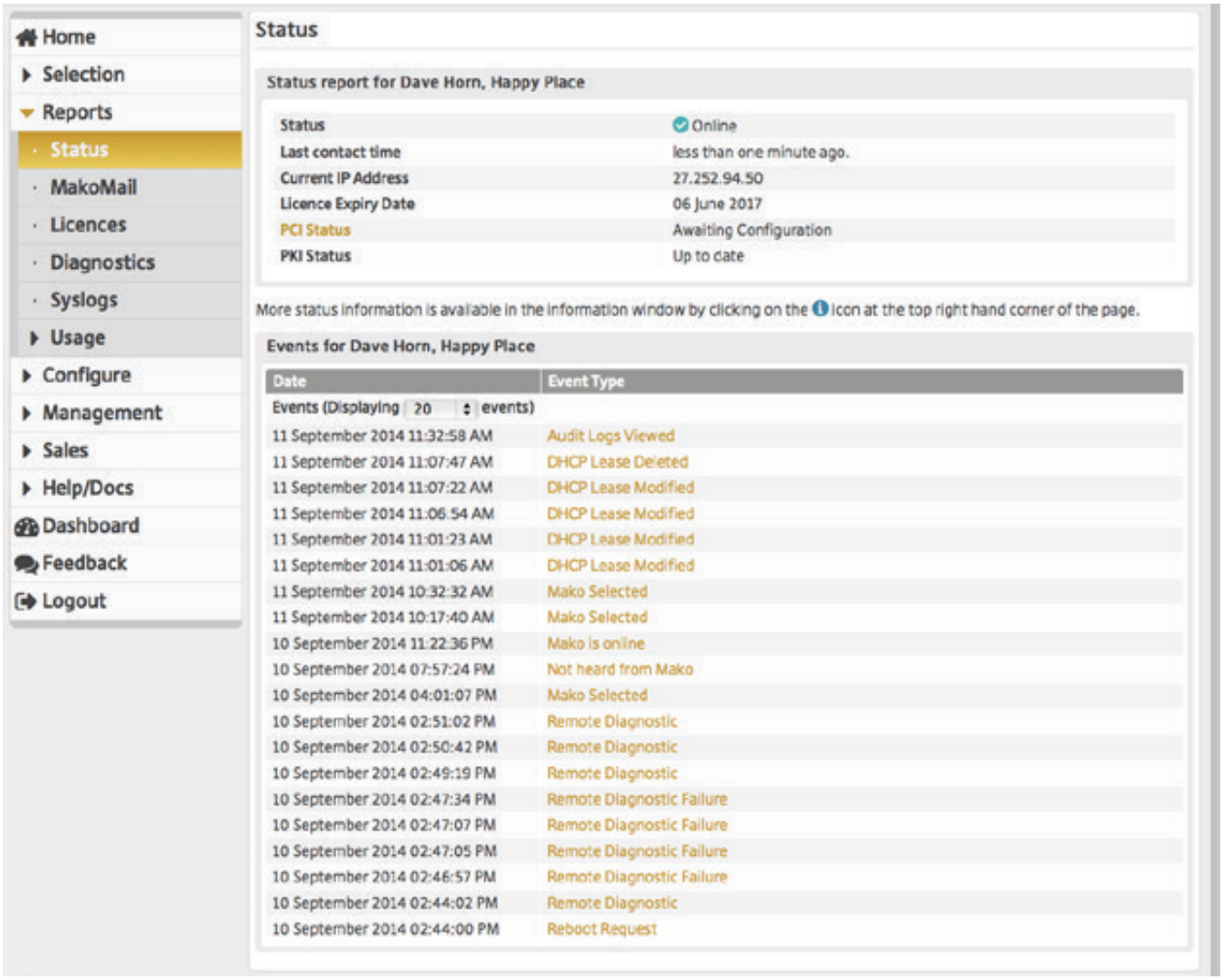


14 DASHBOARD

14 Dashboard

Dashboard is an ongoing ability to present 'widgets' to monitor the performance of your system. It's intended to help service personnel assess network status in custom-designed presentations at-a-glance.

- Click **Create widget**.
- A window presents the choices and presentation types. Design the widget data as required.
- **Submit** when finished. The new widget appears in your browser window.
- Resize widgets by dragging the bottom-right corner of the widget's pane.
- Re-position widgets by dragging them to new locations by the title bar.
- Alter the widget display parameters by clicking the icon.
- Delete the widget by clicking the icon.



15.1 STATUS REPORT FOR [USER, MAKO]

15 Reports > Status

The status report is an overview of the selected Mako. [i]

15.1 Status Report for [User, Mako]

STATUS	Whether or not the Mako is online.
LAST CONTACT TIME	The elapsed time since the Mako last contacted the CMS for configuration updates and log audits.
CURRENT IP ADDRESS	The last assigned public IP address for the selected Mako.
LICENCE EXPIRY DATE	The date at which the selected Mako will not be supported by the Mako System.
PCI STATUS	**Awaiting Configuration:** The PCI Template is not applied to any LAN. **PCI DSS Template Applied:** The PCI DSS Template has been applied to one of the LANs. **PCI DSS Template Modified:** The PCI DSS Template has been applied to a LAN, however changes have been made to it that may bring the LAN out of PCI Compliance.
PKI STATUS	**Up to date:** The Public Key Infrastructure (PKI) key is current. The PKI is a cryptographic technique used for secure communications over insecure networks and changes periodically. **Server key / Host key out of date:** The PKI certificates need to be refreshed.

15.1.1 Events for [User, Mako]

This table displays IP logs for the selected Mako. Clicking on the highlighted text opens a window where details on each event may be inspected.

15.2 > Licences

This simply lists the license-requiring services for the selected Mako. [ii]

---

i Many metrics will not be available if the selected Mako is offline.

ii Mako Failover, while listed as a license, is automatically granted with your service license.

15.3 › Diagnostics

The Diagnostics page lists 25 interrogations on the selected Mako.

ADSL STATUS	Down/Upstream speeds, S/N ratio and associated electrical states.
ARP TABLE LISTING	Address Resolution Protocol Table lists entries for the network.
CELLULAR INFORMATION	Information on the cellular card including IMEI/MEID
CONTENT FILTER RESTART	Issues a restart to the content filter system.
CURRENT CONNECTIONS	Displays all connections to the Mako.
DHCP LISTING	Displays a listing of all DHCP entries.
FAILOVER STATUS	Displays the state of the Failover service.
FIREWALL REFRESH	Refreshes the firewall rules from server.
INTERFACE PING	Pings the host.
LIST PPTP	Lists current PPTP connections.
MAKOSCOPE	Lists several useful states and properties currently.
NETBIOS SCAN	Scans network for NetBIOS names.
REMOTE REBOOT	Reboots the Mako. There is no warning: the Mako will reboot within 2 minutes.
RESET PPP	Resets PPP.
ROUTING TABLE	Lists the routing table.
SOFTWARE CHECK	Forces the Mako to check for new updates.
STORED LOGS	Displays all syslog entries not yet available on the website
VLAN LIST	Lists the VLANs on the selected Mako.
VLAN STATUS	The status of the VLANs on this device.
VPN SETUP	Displays the VPN (IPSec) setup.
VPN TUNNEL DIAGNOSTIC	Displays Tunnel Configuration and Logs.
WLAN AP BASIC SCAN	Scans for and displays nearby wireless access points.
WLAN AP DETAILED SCAN	Scans for and displays detailed information about nearby wireless access points.
WLAN CONNECTIONS	Displays clients connected to the wireless network.
WLAN SYSTEM STATUS	Shows the status of the APs hosted by the CPE, including their channels.

15.4 › Syslogs

System logs are detailed logs of each process request handled by the selected Mako. Logs are listed chronologically, followed by the Name of the process (with the Process Identifier [PID]), and details about the log.

16.1 > MAKO USAGE

16 Reports > Usage

The usage suite of tools creates informative graphs and information breakdowns on the traffic being managed by the Mako. Usage reports have a graph in the top section and the same information in tabular form in the lower section.

16.1 > Mako Usage

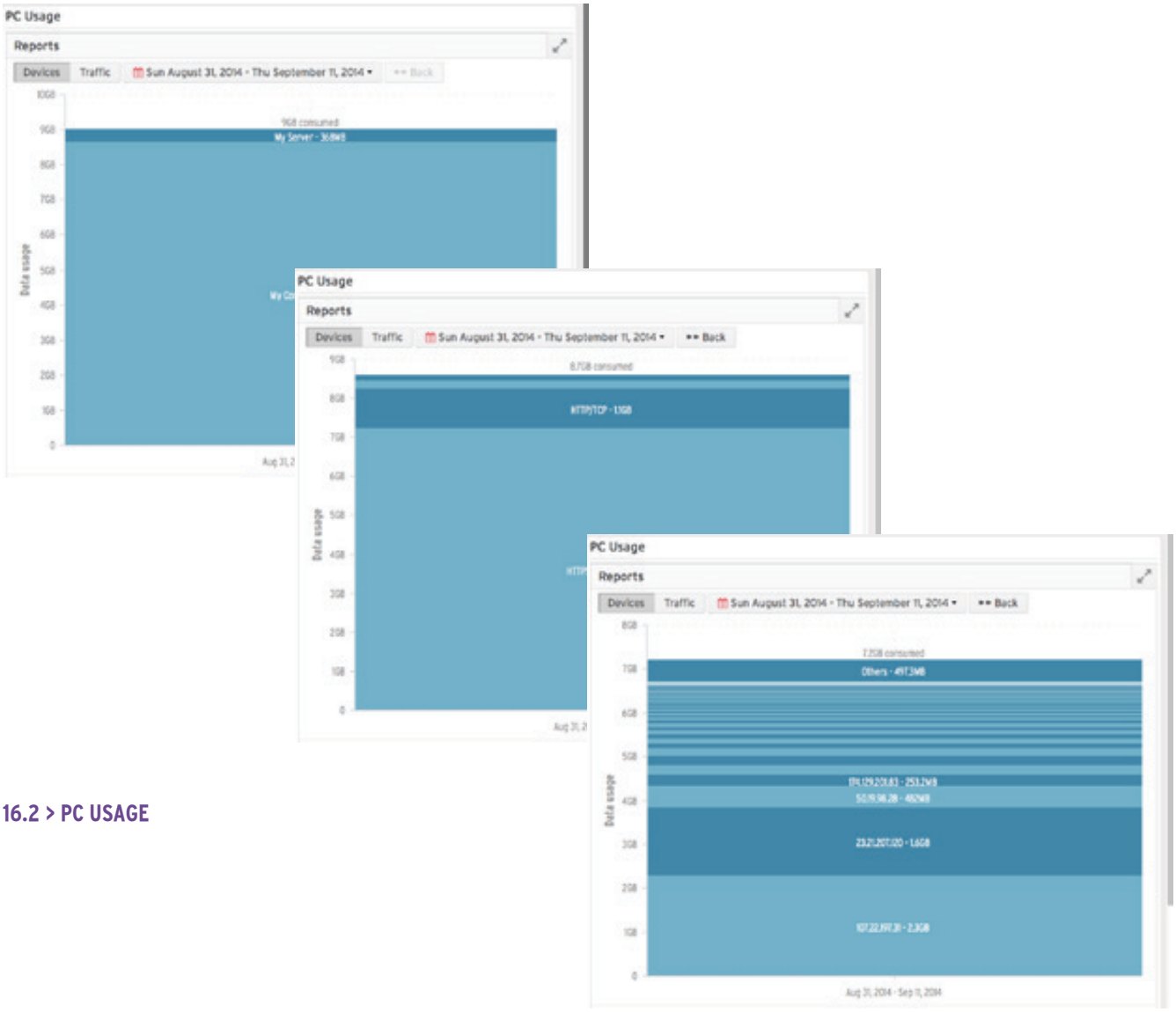
The Mako Usage report gives an interactive overview of the traffic sent and received over the network.

- It displays basic bar graph stats against daily traffic. Daily traffic is measured by the left scale of graph.
- Several horizontal lines mark this Mako's warning threshold the ISP Plan's monthly allocated (free) usage amount, the monthly warning threshold percentage of your monthly allocated traffic, and a line graph tracking cumulative traffic use over the period, as well as a trend line. Monthly traffic is measured by the right scale of graph.
- Hovering the mouse over the graph reveals the day being queried and a magnified view of daily stats.
- Buttons above the main graph allow you to select between showing data for the Primary WAN, Secondary WAN or both, as well as the time period to display.
- Below the graph is a collapsible tabular view of the same information.

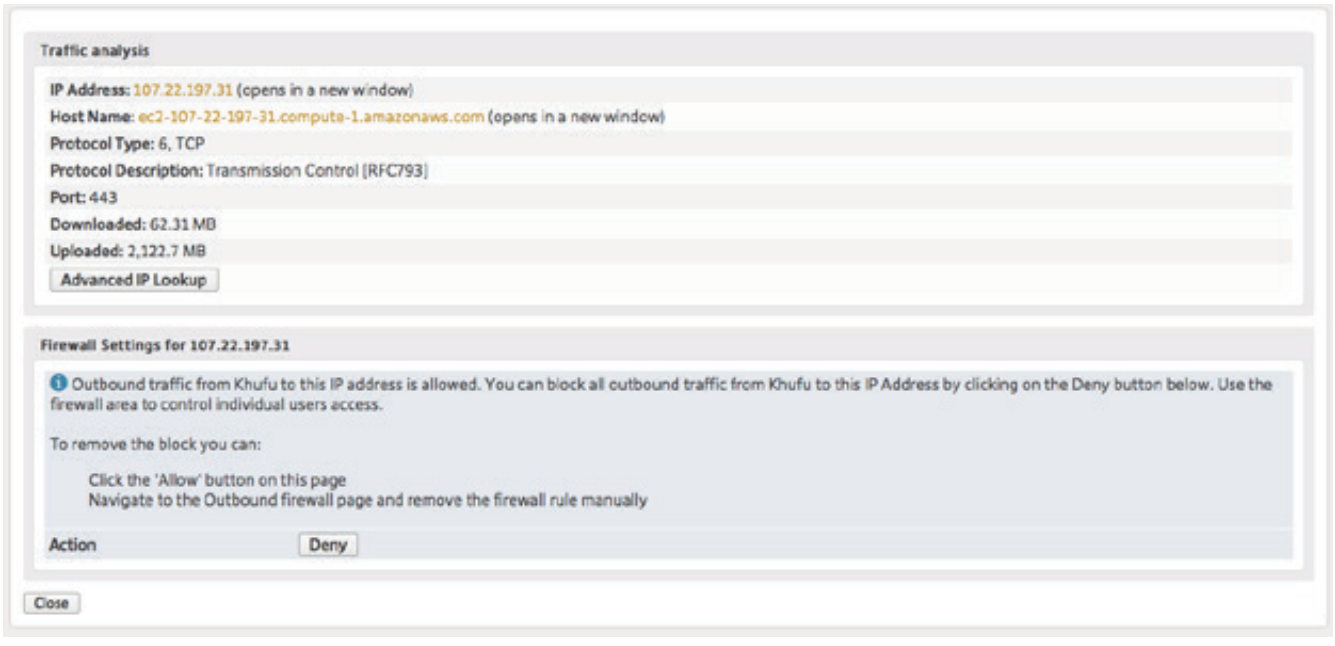
16.1.1 Operating the Usage Graph

You may 'drill down' to finer detail of the Mako's usage by clicking on the appropriate daypart or hourpart of the graph. Depending on the drill-down level, different information will appear.

LEVEL ONE	This is the default view presented for the current month.
LEVEL TWO	Day View. Clicking on a bar of the graph, or the View Chart button in the table, takes you to a 24-hour usage chart. Scaling your browser window will adjust the timescale accordingly.
LEVEL THREE ONWARDS...	PC Usage Chart. This is discussed in the next section. The only difference is that accessing the PC Usage chart through the Mako Usage chart present PC Usage charts inside a modal window. The modal chart may be operated normally, but is dismissed by clicking the ⊗ button, top-right of the window.


PC Usage
Reports
Devices
Traffic
Sun August 31, 2014 - Thu September 11, 2014
Back
Data usage
PC Usage
Reports
Devices
Traffic
Sun August 31, 2014 - Thu September 11, 2014
Back
Data usage
PC Usage
Reports
Devices
Traffic
Sun August 31, 2014 - Thu September 11, 2014
Back
Data usage

16.2 > PC USAGE


Traffic analysis
IP Address: 107.22.197.31 (opens in a new window)
Host Name: ec2-107-22-197-31.compute-1.amazonaws.com (opens in a new window)
Protocol Type: 6, TCP
Protocol Description: Transmission Control [RFC793]
Port: 443
Downloaded: 62.31 MB
Uploaded: 2,122.7 MB
Advanced IP Lookup
Firewall Settings for 107.22.197.31
Outbound traffic from Khufu to this IP address is allowed. You can block all outbound traffic from Khufu to this IP Address by clicking on the Deny button below. Use the firewall area to control individual users access.
To remove the block you can:
Click the 'Allow' button on this page
Navigate to the Outbound firewall page and remove the firewall rule manually
Action
Deny
Close

16.2 › PC Usage

The PC Usage report breaks Internet traffic down by each device on the network. Each device is named either by the device's MAC ID or by an arbitrary name allocated by the user under 6.6 > DHCP Leases.

Each rectangular area in the graph is clickable. Click on each area to drill down to the next level of detail, or click the button **View Chart** in each entry of the lower table.

16.2.1 Devices View

LEVEL ONE	This is the default view, and shows total traffic handled by all devices.
LEVEL TWO	Breaks down the traffic for the clicked device to the ports/protocols used. Generally, this looks like it might have 3-5 sections, but there may be several smaller sections at the top that are not able to be displayed. Check the table in the page's lower section to see a list of all port/protocol traffic.
LEVEL THREE ONWARDS...	Detail list. This page displays all available information about the IP Address, protocol, and amounts of data exchanged over this protocol. **Advanced IP Lookup**: Performs a trace on the IP Address. Firewall Settings for [address]: If you find traffic is coming from, or going to, an inappropriate IP Address for this network, clicking the **Deny** button automatically sets a Deny rule for this IP Address.

16.2.2 Download CSV

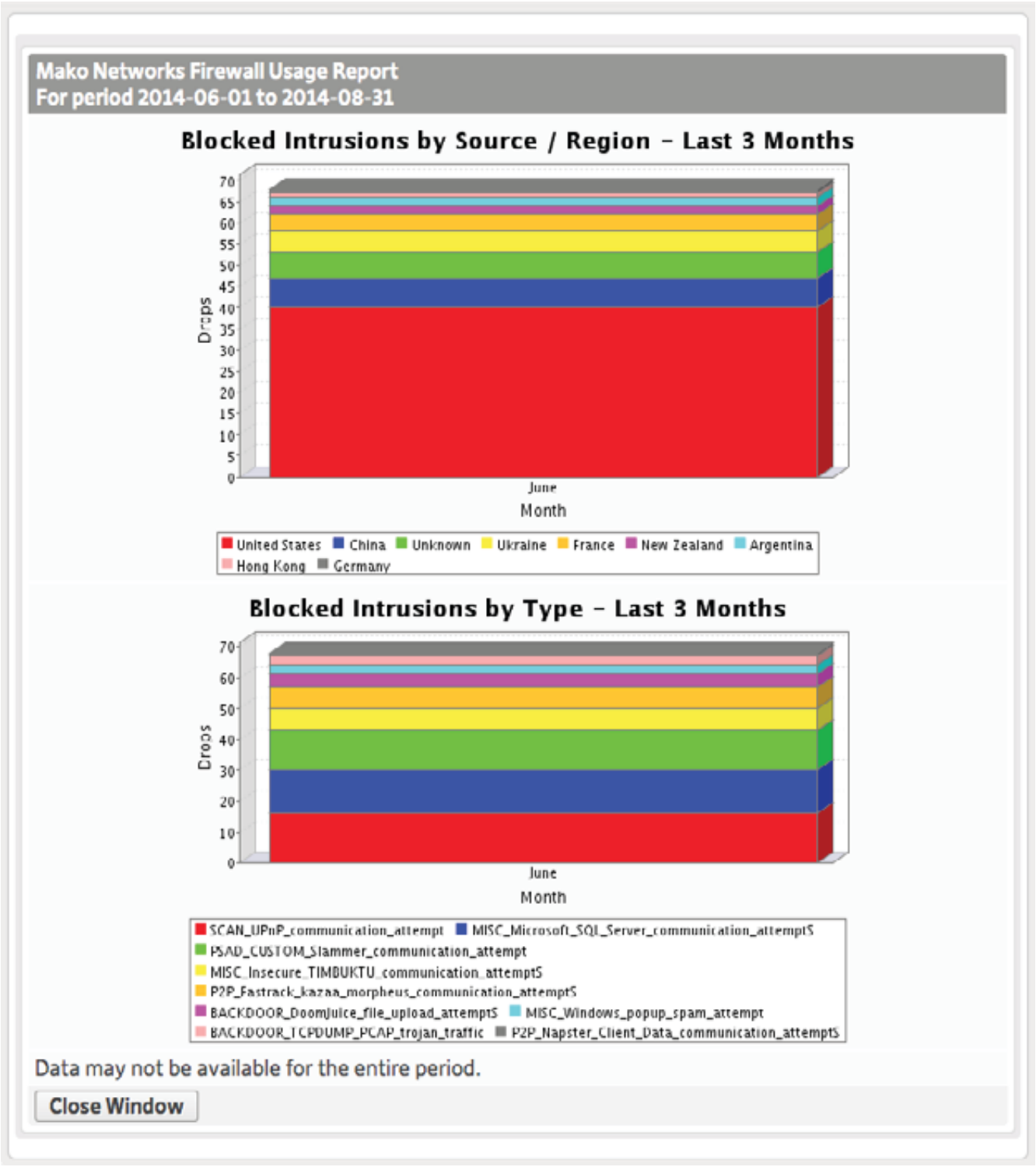
This button converts the current level of data presented into a list of Comma Separated Values. CSV files may be opened in most spreadsheet applications as a table.

16.3 › Remote Access

This page (which should be more accurately named "PPTP Access") reveals any activity made by PPTP VPN users of the local network. Once the date range for the usage stats is selected you will be presented with a piechart and table of logged usages. i

USERNAME	The VPN Username
CONNECT TIME (UTC)	The time (Coordinated Universal Time) at which access occurred.
DURATION	The duration of access.
TOTAL	Amount of data exchanged.
SOURCE IP	The public IP address over which the VPN tunnel was created.
FLAG	The calculated national flag associated with the IP Address.

i Due to the nature of IPSec's security protocol, IPSec connections cannot be reported.



16.5 > SHARKNETIDS

16.4 › Guardian Usage

Guardian is the Mako System's Web Access Control system. i The report consists of a simple pie chart indicating the sites most processed by Guardian and a detailed table of sites processed.

URL	The domain accessed.
TRAFFIC (MB)	The amount of traffic accessed.
REQUESTS	The number of times this web pages in this domain has been accessed.
% ALLOWED	The number of requests for data denied, divided by the total amount of requests

This list is downloadable as a CSV file

16.5 › SharkNetIDS

The Mako System incorporates a set of intrusion detection and reporting tools for analysing unsought connections and suspicious digital activity. If an unauthorized intrusion is detected the connection is dropped, so the reports are measured against dropped connections.

- Once a date range has been selected, this section presents two bar graphs.
- Hovering over any bar graph section reveals the exact number of dropped connections attributed to intrusions.
- Clicking on any bar graph takes you to a pie chart representation of the same data with an accompanying table.

i A separate license is required to use Mako Guardian with the Mako System. For more about Guardian consult the Guardian Manual.

17 Overview

The Mako System offers a cloud-managed, turnkey solution to create broadband networks for small sites. With anytime, anywhere access, the Mako System offers real-time management, reporting and proactive security in one solution.

The Mako System is a combination of 2 parts: a network appliance (the Mako) and cloud-based Central Management System (CMS). These components work together to provide a complete network connectivity and management service, enabling you to connect, protect and control your network(s).

Mako Appliances

Mako appliances offer the choice of WAN interfaces including Cellular, Ethernet and ADSL2+. There is a Mako to suit any small site's requirements, and Mako Virtual Private Network (VPN) concentrators can link them back to a central or corporate network (see separate hardware appliance specifications for specific details). Mako appliances ship with proprietary software incorporating a default configuration, which enables them to connect to the Internet, communicate with the CMS and retrieve their customer-specific configuration. Once online, Makos connect directly to the Internet and communicate regularly with the CMS using a patented communication method.

The Unique Central Management System

The Mako CMS is accessed via a secure website that users log into to manage their network(s). A user's login gives them access to all their Makos around the world, providing a central place from which to manage their complete network.

You or your designated IT Professional have 24-hour secure remote control over your connection(s) to the Internet or connections between sites with this CMS. The CMS allows you to modify firewall rules, connect sites via VPNs, check usage patterns and even change your network's IP addressing.

Patented Communication Method

Mako appliances make it possible to have a hosted, cloud-based management system that receives traffic information from individual Mako appliances and then analyses, interprets and reacts to that information. The communication method eliminates the need for on-site configuration, with authenticated users accessing the CMS via the Internet to interact with their Mako appliances.

Unlike traditional management platforms, communication with the management system is initiated by the end-point, thus negating the need for static IP addresses and individually pre-configured appliances. Every 2 minutes, each Mako appliance checks with the management system if there is a need for configuration changes or firmware updates. The appliance also transmits raw traffic logs to the CMS for automatic interpretation and analysis.

Robust Security

Your networks are always updated and guarded through automatic software updates and patches, while intrusion attempts are managed in real time. The stateful inspection firewall performs a comprehensive analysis of all traffic entering and leaving your networks to uphold your network's integrity.

Firewall

Your firewall, a key security item, guards against unwanted information from entering or leaving your network. Your Mako's stateful packet inspection firewall not only examines packets of information, but makes

decisions based upon information derived from multi-layered communications and other applications, providing comprehensive, enterprise-level protection.

With the CMS you have authoritative control over traffic entering and leaving your networks.

PCI Compliance

The Mako System is powered by Mako Networks Ltd, a certified **Payment Card Industry Data Security Standard (PCI DSS) Level 1 Networking and Security Service Provider**. This means that you can easily meet the requirements of PCI DSS compliance.

The PCI DSS rules have been designed to protect banks, merchants and cardholders from falling victim to credit card fraud. PCI DSS outlines how a merchant should protect their point of sale network and ensures security is maintained on an ongoing basis.

The Mako System lowers the cost and complexity of PCI DSS compliance by automating network security and nearly every other process of a merchant's PCI DSS compliance.

With proactive alerts, merchants using the Mako System cannot mistakenly put themselves at risk of non-compliance. Any attempt to inappropriately modify the network configuration will generate a warning and require the user to confirm the modification by entering an authorising password.

Through Mako Networks, Mako provides a QSA-designed website which can deal with almost all remaining aspects of merchant PCI DSS (documentation, policy and process), leaving the merchant only having to take care of physical security.

The Mako system is the solution for card-present merchants transacting over IP, providing peace of mind to cardholders, merchants and their banks. The Mako System enables a merchant to more easily comply with all of their PCI DSS obligations. Many merchants lack the technical knowledge required to correctly implement the PCI DSS requirements and buying in that experience is expensive using traditional solutions.

VPN

Virtual Private Networks allow you to assign secure remote access to your networks over the Internet.

Linking 3 or more Mako-protected networks is just as easy. The CMS allows this to happen without static IP Addresses. In the same way you can also allow specified users remote access to your Mako-protected networks with the Remote VPN feature – A useful feature for accessing your networks whether you're home or away.

Proactive Alerts

The Mako CMS automatically provides proactive alerts for extraordinary usage, unit offline, worm detection and hardware triggers such as fan speed and CPU temperature. The CMS also sends monthly reports on usage, intrusion attempts and easy-to-read company-wide summaries for end-users with multiple sites.

Logging/Reporting

While all traffic from your Mako goes directly out onto the Internet, your Mako sends traffic information securely to the CMS. This analysis gives you the ability to monitor and control your Internet usage, using any PC from any worldwide location. Simply log onto the CMS to see how your business's broadband Internet connection is being used, by whom and whether this was for personal or business use, monitor where PCs on your network have been going and much more.

24-Hour Remote Control

Because your Mako uses the CMS, you or your designated IT Professional have 24-hour secure remote control over your connection to the Internet. Via the CMS you can modify firewall rules, create and disable VPNs, check usage patterns and even change your networks IP Addressing.

Automatic Updates

Mako automated software and firmware upgrades mean that new services and increased functionality are added to the platform on an ongoing basis. Mako software is proactively patched and updated immediately upon authentication and availability, providing unparalleled reliability and security without manual intervention. You can be assured that your Mako appliance will continue to be current as long as it has a current licence.

Diagnostics

Mako Diagnostics gives support personnel the ability to remotely resolve network and connectivity issues without the need for on-site visits or technically literate users.

Mako Diagnostics reduces support costs by allowing the helpdesk to very quickly identify and resolve problems all the way to the Mako appliance level.

Optional Feature Enhancements

The Mako System has facilities for incorporating optional feature enhancements such as Advanced Content Filtering, Email laundering, spam and virus protection. New features and options are implemented when necessary through automatic updates.

Make sure you keep up to date by regularly logging into your CMS.

A Glossary

ADSL

Asymmetric Digital Subscriber Line. A group of technologies used to transmit high speed (broadband) data across a non-digital telephone circuit, with the channel capacity towards the subscriber being several times greater than that from the subscriber. Typical bandwidths are in megabits per second.

Browser

A software application that displays HTML formatted text and facilitates access to websites. Examples are Internet Explorer, Safari and Firefox. The application provides the web browsing service, based on the HTTP protocol.

CMS

The Mako Central Management System is simple to use and takes the normally complex tasks of network management and makes them easy. The CMS essentially takes traffic information across your network gateway, analyses it, automatically fixes any issues and then reports to you what was wrong. Any issues that require your intervention can be simply addressed online.

The types of things that a business will be alerted to are:

- Extraordinary usage
- Worms
- Broadband data usage
- Broadband traffic limit reached
- Licence expiry
- Dynamic DNS activity
- Mako temperature

CPE

The Mako appliance may also be referred to as the Customer Premise Equipment (CPE).

DHCP

Dynamic Host Configuration Protocol. This system allows IP addresses in a network to be assigned automatically on machine power up. The IP address may change from one network session to the next.

DMZ

Demiliterized Zone. A term taken from the armed forces, a DMZ in network context is a separate network zone that is intended to provide limited external access to internal services without exposing the core network to risk from attack. For example, if you have a local publicly accessible web server, it should be placed in a DMZ rather than residing on the office network.

DNS

Domain Name Service. This service resolves host names to IP addresses.

A DNS service provides your network a 'fixed' address on the Internet without the need for a static IP address. Once you have an account with either of our 2 support Dynamic DNS providers, they will give you a domain name. The Mako will then update the provider with its current public IP address so the domain name references the correct address. This way the domain name remains static and has the IP address it references updated automatically by the Mako System.

To sign up to one of these services, follow the instructions and documentation on the provider's website. You'll receive a username and password from your Dynamic DNS provider. Enter these in the appropriate section on the Mako Networks Dynamic DNS screen. Once entered, each time your Mako changes its public IP address, it will update your Dynamic DNS provider.

Email

A software application for the construction and transmission of SMTP messages. Examples are MS Outlook, Thunderbird and Apple Mail.

Ethernet

Ethernet is the most widely installed local area network (LAN) technology. Specified in a standard, IEEE 802.3, Ethernet was originally developed by Xerox and then developed further by Xerox, DEC, and Intel. An Ethernet LAN typically uses special grades of twisted pair wires such as CAT5 or CAT5e.

Firewall System

A firewall prevents unwanted Internet services from coming into or leaving the office network. It's a technological barrier designed to prevent unapproved or unwanted, possibly destructive, communications between computer networks or servers and hosts. A firewall filters the information coming through the Internet connection into your private network or between computer systems in an internal network. If an incoming packet of information is flagged by the filters, it is not allowed through.

In short, it provides a strong, first line of defence from the following types of attacks:

- **Remote login**
  remotely control your computer and access sensitive files.
- **Application backdoors**
  a hacker capitalises on the flaws with remote access in some applications.
- **SMTP session hijacking**
  gaining access to your email contacts and using these for the purposes of spam.
- **Operating system bugs**
  similar to application backdoors, but through the operating system in this case.
- **(Distributed) Denial of Service (DDoS)**
  essentially crippling your office system or server by sending a multitude of bogus requests for non-existent connections.
- **E-mail bombs**
  Thousands of emails are sent to your inbox, incapacitating your email system.
- **Macros**
  A macro is usually used to simplify tasks by bundling a series of commands into one action. However hackers have exploited these, using them to perform a series of malicious commands on your computer.
- **Viruses**
  A well-known threat that is self-replicating and can spread throughout your network causing minor to major damage.
- **Spam**
  More of a hindrance than a threat, however some can contain links to malicious websites.
- **Redirect bombs**
  Hackers can redirect the path information takes by sending it to a different router. A method used for denial of service attacks.
- **Source routing**
  Generally information (packets) moves through the Internet and local networks with the aid of routers. However the specific route is randomly determined by the source. Hackers mimic this behaviour to make

the information appear as though it originated from a trusted source. To resolve this problem, source routing is disabled by your firewall.

FTP

File Transfer Protocol. This is a service for bulk data transfer over the Internet.

Gateway

A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.

GRE Tunnel

Generic Routing Ecapsulation Tunnel. A secure way for IP traffic to be carried through a network, typically used for VPN connections.

HTML

Hyper Text Markup Language. A standard that defines how to format text, graphics, etc., on a web page for display on a Browser.

HTTP

Hyper Text Transfer Protocol. The service which transfers HTML formatted web pages to a Browser.

Hub

In general, a hub is the central part of a wheel where the spokes come together. In data communications, a hub is a place of convergence where data arrives from one or more directions and is forwarded out in all directions (along all the spokes). This extends the connectivity of an Ethernet LAN (local area network) to provide for additional computer connections. This concept is fine in smaller LANs but may cause congestion in larger LANs, where a switch (which directs the traffic) would be more applicable.

IPsec

An standard protocol for establishing secure virtual private networks (VPNs) Over IP networks .

ICMP

Internet Control Message Protocol. An integral part of the Internet Protocol suite that handles error and control messages. Specifically, routers and hosts use ICMP to send reports of problems about datagrams back to the original source that sent the datagram. ICMP also includes an echo request/reply used to test whether a destination is reachable and responding.

IP

The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognises the packet as

belonging to a computer within its immediate neighbourhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

IP Address

In the most widely installed level of the Internet Protocol today (IPv4), an IP address is a 32-bit number that identifies each host on the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

An IP address has 2 parts: the identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. On the Internet itself, that is, between the router that move packets from one point to another along the route only the network part of the address is looked at.

LAN

A local area network is a group of computers and associated devices that share a common communications line or Wireless link. Typically, connected devices reside in a small geographic area (for example, within an office building). A LAN may serve as few as 2 or 3 users (for example, in a home or small office network) or as many as thousands of users.

MAC address

Media Access Control. The unique hardware address of a machine's connection to a local area network. Each NIC has a unique MAC.

NAT

Network Address Translation, an Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

NIC

Network Interface Card. The component of a computer that allows connection to a LAN (local area network).

Packet

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, Graphics Interchange Format file, Uniform Resource Locator request, and so forth) is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).

Port

The number that identifies a specific channel for communications relating to a specific Service. Ports greater than 1024 are called ephemeral ports—these are for assignment to proprietary or special purpose applications.

PPTP

The Point-to-Point Tunnelling Protocol is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. PPTP has been the subject of many security analyses and serious security vulnerabilities have been found in the protocol.

Router

A communications device connected between 2 (or more) different networks, which maps (routes/directs) traffic between the IP addresses on each network.

Service

Services comprise 3 elements—a pair of communicating software applications; the definition of the data structures which the applications exchange; and the definition of the protocols by which the applications exchange data structures. Established services include FTP, Telnet, HTTP, SMTP, etc. There are also proprietary or special purpose services.

SMTP

Simple Mail Transfer Protocol. The service for encapsulating and sending messages to another person on the Internet, known as Email.

SSH

Secure shell. A special program providing a secure communications channel between SSH client and SSH server processes.

Switch

An Ethernet connectivity device, similar to but more advanced than a Hub, which partitions traffic between connected computers to lessen congestion.

On an Ethernet LAN a switch determines from the physical device MAC address in each incoming message frame, to which output port it is forwarded.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).

Telnet

A service which provides remote terminal login to a multi-user host.

VLAN

VLAN's provide a function for separating users into groups through network segments. This is done virtually and eliminates the need for physical hardware changes and configurations. This means that only one switch can be used for creating separate "virtual" LANs on this one physical hardware device. For instance, on a 24-port switch, you can create 3 isolated VLANs of 8 users each.

VLANs can also span over multiple switches, i.e. 2 users on one switch and 3 users on another using VLAN Trunking.

VLAN Trunking

More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for various VLANs.

Grouping computers located in disparate locations by VLAN can simplify a network design. A VLAN is essentially the same as a local area network (LAN), but it allows for easier grouping of computers even if they're not on the same network switch.

VLAN memberships are configured through a software interface, as opposed to physically moving cables on switches. Most enterprise-level networks today use the concept of VLANs.

Without VLANs, a switch considers all interfaces on the switch to be in the same broadcast domain.

VPN

A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one company. The goal of a VPN is to provide the company with the same capabilities, but at a much lower cost.

Web, or World Wide Web

The World Wide Web is a system of interlinked documents, images and other media hosted by multiple servers across the Internet and accessed via web browsers.

MRU: The Maximum Receive Unit (MRU) is the size of the largest packet the Mako will accept. Increasing the MRU means larger incoming packets, which in turn increases transmission errors as the whole packet must be retransmitted. The recommended minimum is 250 and maximum is 1500.

Encapsulation: Choose the encapsulation type from the drop down menu, Virtual Concatenation (VC) or Logic Link Control (LLC).

Plan Realm: Enter the URL of the ISP here.

IP Range Support: Check this box for IP Range Support.

Domain Prefixing: Check this box for Domain Prefixing.

Business plan: Check this box for Business Plan.

Bandwidth (Kbits/sec) Down: Leave this at 0 to let the Mako automatically decide this. To manually override this enter the value here.

Kbps Up: Leave this at 0 to let the Mako hardware automatically decide this. To manually override this enter the value here.

Cellular: Check this box if the ISP provides Cellular services.

1 Warranty

1) **Standard Limited Warranty.** If the products purchased hereunder are resold by a distributor or reseller to an end-user (customer) pursuant to the terms hereof in their original, unmodified, unused condition, Purchaser shall pass on to its customers, or keep as applicable for internal use, the MAKO NETWORKS LTD. standard limited warranty for the products, as summarized in documentation supplied with the product and including provisions and limitations set forth below. The Manufacturer warrants the Mako Appliance for one (1) year. The Warranty begins on the date of purchase as shown on your providers invoice.

2) **Express End-user Limited Warranty.** Each MAKO NETWORKS LTD. product purchased hereunder is warranted against defect in material and workmanship and will substantially conform to MAKO NETWORKS LTD. product documentation for the period set forth in the documentation supplied with the product following delivery to end-user (the "Warranty Period"). This warranty extends only to end-user and will not extend to, nor may it be assigned to, any subsequent user, Purchaser or user of a MAKO NETWORKS LTD. product, whether such MAKO NETWORKS LTD. product is alone or incorporated into end-user's product.

3) **Exclusions.** The express warranty set forth above is contingent upon the proper use of a MAKO NETWORKS LTD. product in the application for which it was intended and will not apply to any MAKO NETWORKS LTD. product that has been (i) damaged during shipping, (ii) modified or improperly maintained or repaired by a party other than MAKO NETWORKS LTD. or its designees, or (iii) subjected to unusual physical or electrical stress. This includes operation of the product outside the Operating Specifications of the product.

4) **Limitation of Remedy.** In the event a MAKO NETWORKS LTD. product fails to perform as warranted, MAKO NETWORKS LTD. sole and exclusive liability and end-user's only remedies for breach of this warranty shall be, at MAKO NETWORKS LTD.'s option to repair, replace or credit an amount not exceeding the Purchaser's purchase price of each product found to be defective, provided that:

   4.1) **End-user complies with the rejection and warranty procedures contained in Section 5 below and returns the MAKO NETWORKS LTD.** product that the end-user considers defective for examination and testing.

   4.2) **MAKO NETWORKS LTD.** shall not be liable under this warranty if testing and examination by MAKO NETWORKS LTD. discloses that the MAKO NETWORKS LTD. product has been modified or altered in any manner after it was shipped by MAKO NETWORKS LTD.

   4.3) **MAKO NETWORKS LTD.** shall not be liable under this warranty if testing and examination by MAKO NETWORKS LTD. discloses that the alleged defect in the MAKO NETWORKS LTD. product does not exist or was caused by end-user or any third person's misuse, neglect, improper installation or testing, unauthorized attempts to repair or any other cause beyond the range of intended user, or by accident, fire or other hazard.

   4.4) **MAKO NETWORKS LTD.** shall not be liable under any warranty under this Agreement with respect to any MAKO NETWORKS LTD. product that is not returned in its original shipping container or a functionally equivalent container.

   4.5) **If MAKO NETWORKS LTD.** testing and examination does not disclose a defect warranted under this Agreement: MAKO NETWORKS LTD. shall so advise Purchaser and dispose of such MAKO NETWORKS LTD. product in accordance with Purchaser's instructions on behalf of end-user and at Purchaser's cost.

Support
support@makonetworks.com

Web site
www.makonetworks.com