

Changing EdgeMarc Administration Security Settings

Date: October 2014

U.S. Headquarters:

Edgewater Networks, Inc.
5225 Hellyer Ave. #100
San Jose, CA 95138

Phone: 408.351.7200
Fax: 408.727.6430
edgewaternetworks.com

© 2014, Edgewater Networks, Inc.

Edgewater Networks Confidential, All Rights Reserved.

Trademarks

EDGEWATER NETWORKS EDGEMARC®, EDGEPROTECT®, and EDGECONNECT® are registered trademarks of Edgewater Networks, Inc. EDGEWATER NETWORKS™ and EDGEVIEW™ are trademarks of Edgewater Networks, Inc. Any other trademarks appearing in this manual are owned by their respective companies.

Copyright

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Edgewater Networks, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement of the implied warranties of merchantability or fitness for a particular purpose.

Export Notice

You (Purchaser) acknowledge that these products are subject to the U.S. Export Administration Regulations (the “EAR”) and that you will comply with the EAR. You are not located in Cuba, Iran, North Korea, Sudan, and Syria. You will not export or re-export this product, directly or indirectly, to: (1) any countries that are subject to US export restrictions (currently including, but not necessarily limited to, Cuba, Iran, North Korea, Sudan, and Syria); (2) any end user who you know or have reason to know will utilize them in the design, development or production of nuclear, chemical or biological weapons, or rocket systems, space launch vehicles, and sounding rockets, or unmanned air vehicle systems; or (3) any end user who has been prohibited from participating in US export transactions by any federal agency of the US government. In addition, you are responsible for complying with any local laws in your jurisdiction which may impact your right to import, export or use these products.

Licensing

Use of this product is subject to Edgewater Networks Software License Agreement.

Portions of this product include software sponsored by the Free Software Foundation and are covered by the GNU GENERAL PUBLIC LICENSE.

See the http://edgewaternetworks.com/support/licenses/ for more information regarding licenses.

Warranty

Product warranty does not apply to damage caused by lightning, power surges, or wrong voltage usage.

Typographical Errors

This publication could include technical inaccuracies or typographical errors, for which Edgewater Networks never can or shall be held liable. Changes are made periodically to the information herein; these changes will be incorporated in new releases of this publication. Edgewater Networks may make improvements or changes in the product or products described in this publication at any time, without prior notice.

Document Release Date

9/22/14

Contents

Changing EdgeMarc Administration Security Settings 1

Accessing the EdgeMarc Web Configuration Interface 1

Changing the Administrative and Read-Only Passwords 4

Changing the CLI Password 5

Configuring Firewall Settings 6

Enabling HTTPS Access 8

Defining Trusted Hosts 8

Restricting Access to the Management Interface 9

Configuring an HTTPS Certificate 11

Deploying the EdgeMarc 11

1

Changing EdgeMarc Administration Security Settings

This document describes how to change EdgeMarc administration default settings to ensure maximum security for your system. It also includes procedures for configuring firewall settings and defining trusted hosts to further secure your device. The following topics are covered.

Accessing the EdgeMarc Web Configuration Interface

Changing the Administrative and Read-Only Passwords

Changing the CLI Password

Configuring Firewall Settings

Enabling HTTPS Access

Defining Trusted Hosts

Restricting Access to the Management Interface

Configuring an HTTPS Certificate

Accessing the EdgeMarc Web Configuration Interface

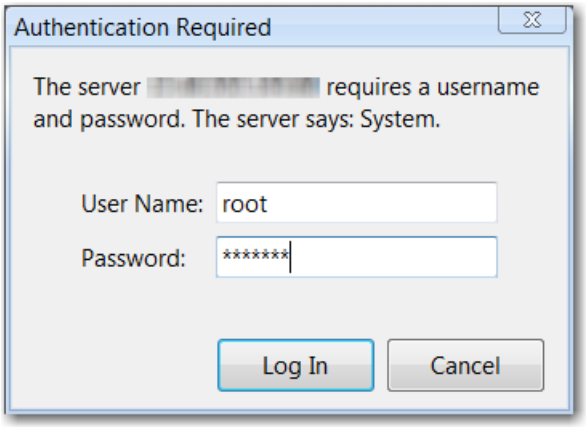
You'll need to access the EdgeMarc web configuration interface to configure the EdgeMarc as follows:



Note
The following steps assume that the EdgeMarc is using the factory default settings.

1. Connect a computer to the LAN port on the EdgeMarc.
2. Enable DHCP on the computer so that it will obtain an IP address.
3. Launch a web browser on the computer and enter the URL string: **192.168.1.1**.
4. Press **Enter.** The login window opens.

© 2014 Edgewater Networks, Inc. All rights reserved.



5. Enter the following credentials:

   User name: **root**

   Password: **default**

   The **System** window opens.

Note

If the **System** window does not open and "message of the day" displays, select **System** from the **Configuration Menu** to open the System window.

Note

The following example shows the System screen for the EdgeMarc 45xx series, devices running version 11.6.13 software. Your System screen may look different, depending on your EdgeMarc model and software version.

© 2014 Edgewater Networks, Inc. All rights reserved.





To maintain system security, change the following passwords from the default:

- GUI administrative password
- GUI read-only password
- CLI password (call Edgewater Technical Support to obtain the CLI password)

You should also set additional security parameters. Refer to Configuring Firewall Settings for more information.

© 2014 Edgewater Networks, Inc. All rights reserved.

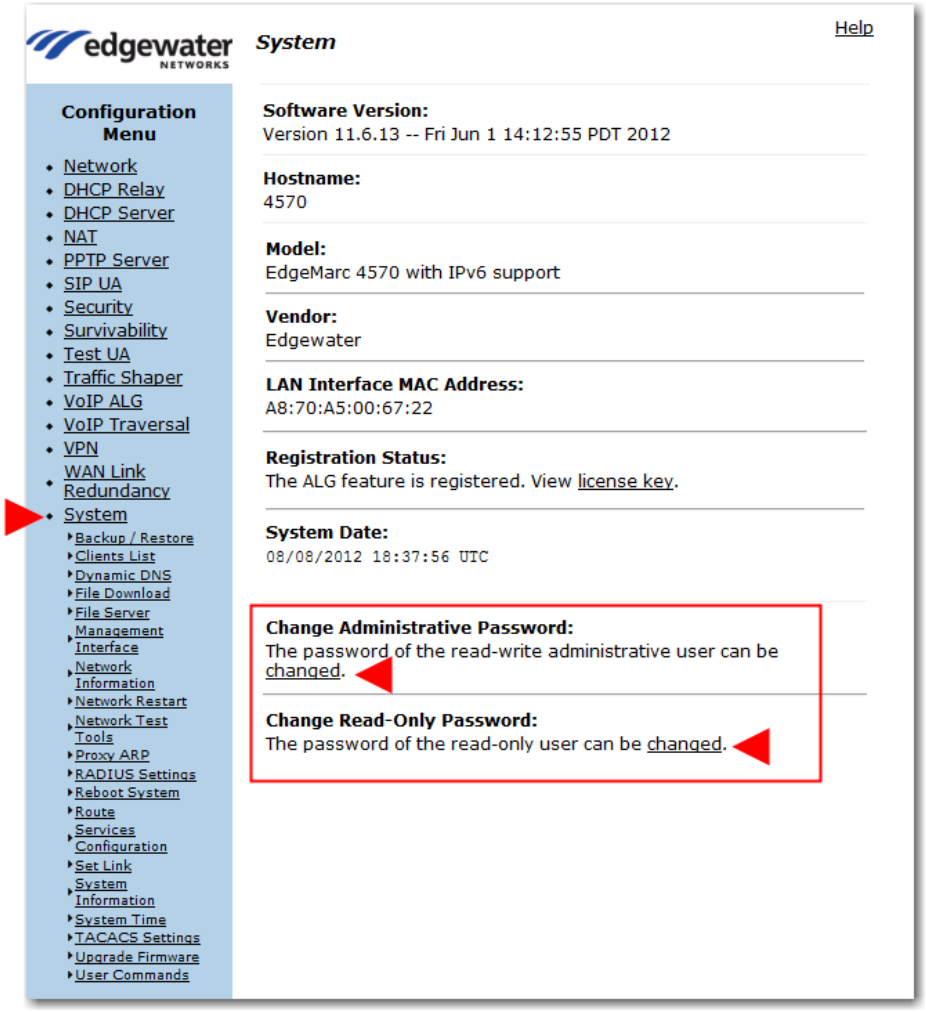
Changing the Administrative and Read-Only Passwords

The first time you log in to the web GUI, change the Administrative password and the Read-Only password for the EdgeMarc. Each password must be between 6 and 8 characters and contain at least one uppercase character and at least one number. It should not be a dictionary word.

Note

The Administrative password and CLI password should not be the same.

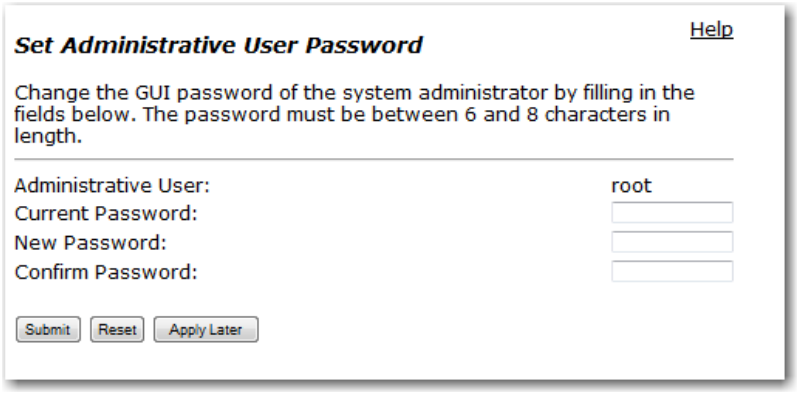
To access the System page in the EdgeMarc web user interface and change these passwords, click **System** in the **Configuration Menu**.



To change the Administrative password:

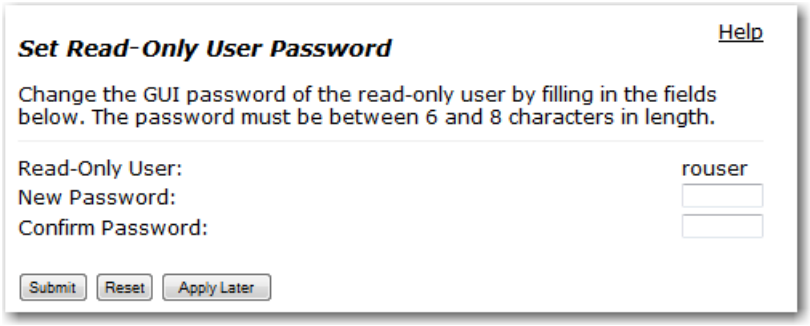
1. On the **System** page, click **Changed** under Change Administrative Password.
2. Enter and confirm the new password.
3. Click **Submit**.

© 2014 Edgewater Networks, Inc. All rights reserved.



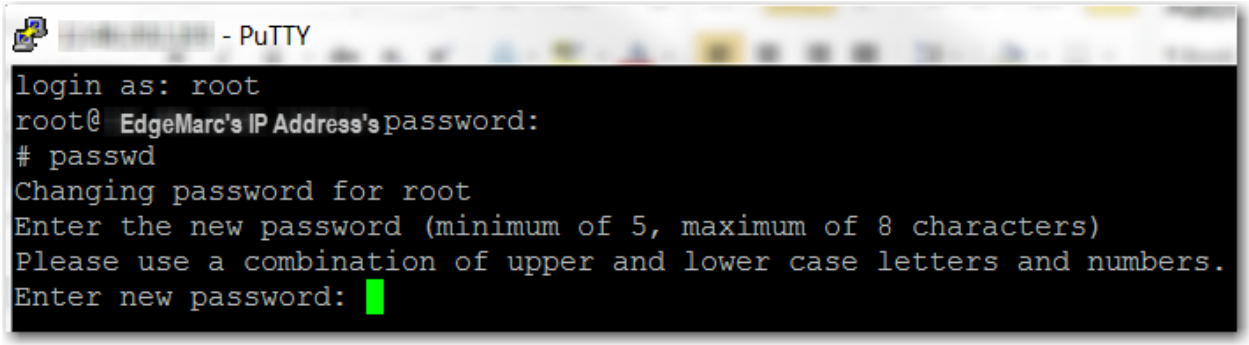
To change the Read-Only password:

1. On the System page, click Changed under Change Read-Only Password.
2. Enter and confirm the new password.
3. Click **Submit**.



Changing the CLI Password

1. Obtain the CLI password from Edgewater Networks Technical Support.
2. Access the CLI on your EdgeMarc (using telnet, ssh, or a serial connection).
3. Login as root.
4. Enter the CLI password and press Enter.
5. At the # prompt, type **passwd** and press Enter.

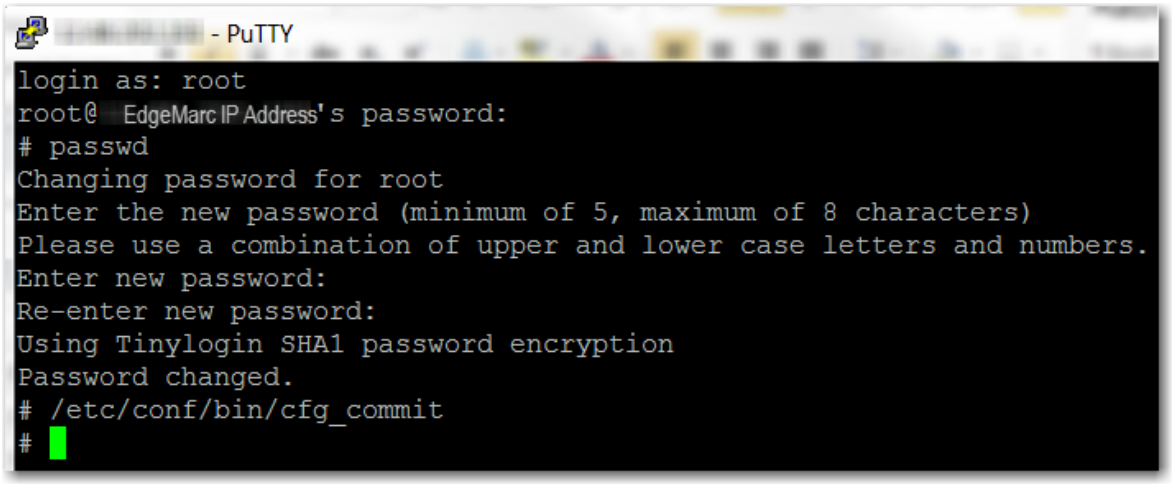


© 2014 Edgewater Networks, Inc. All rights reserved.

6. Enter a new password with a minimum of 5 characters and a maximum of 8 characters). Use a combination of uppercase and lowercase letters and numbers. Press Enter.

Note
The Administrative password and CLI password should not be the same.

7. When prompted, retype the new password and press Enter.
8. Type **/etc/conf/bin/cfg_commit** and press Enter to save the changes and commit to flash.



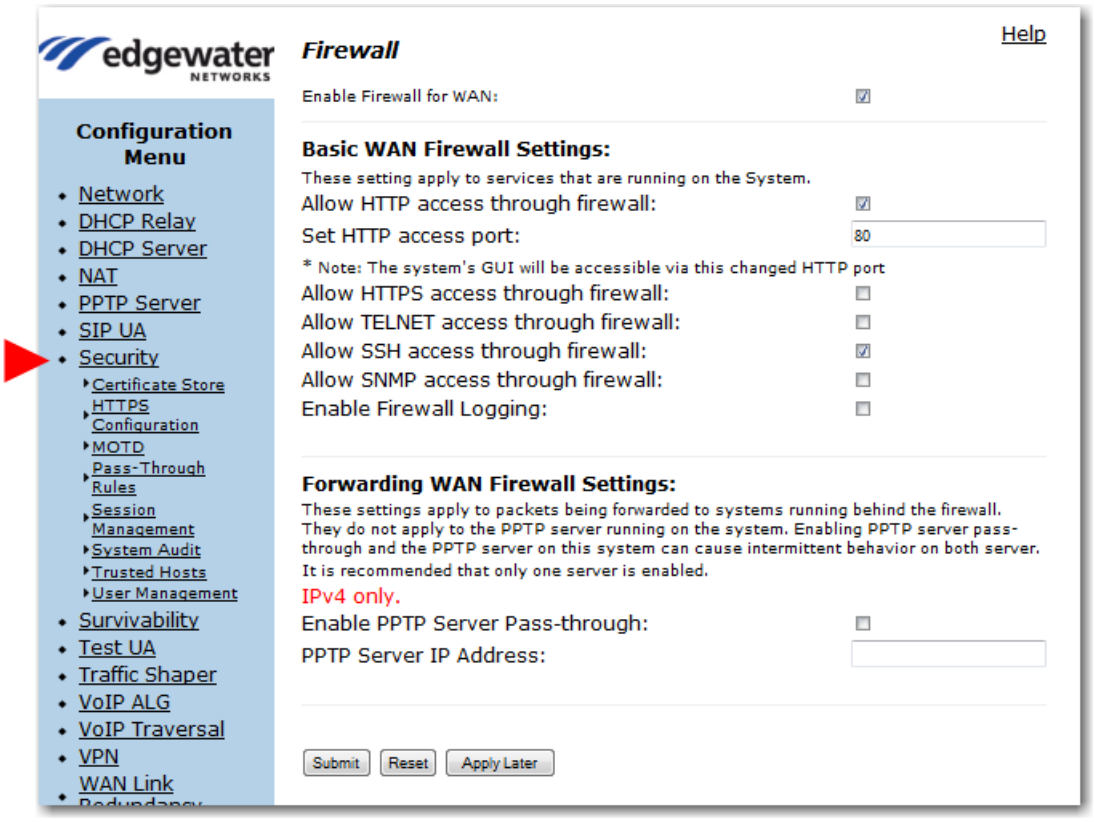
Configuring Firewall Settings

The EdgeMarc can act as a firewall for voice, video and data traffic. You can define policies to filter traffic that traverses the device or administration traffic destined to the device.

Use the following procedure to define firewall policies for data traffic. Voice and video firewalls are implemented by VoIP Proxy. For more information on VoIP Proxy functions and configuration, view the help link on **VoIP ALG** page in the web interface.

1. Select **Security** from the Configuration Menu. The Firewall page opens.

© 2014 Edgewater Networks, Inc. All rights reserved.



2. Check the **Enable Firewall for WAN** checkbox. This is disabled by default.
3. Select protocol and port options for the WAN firewall in the **Basic WAN Firewall Settings** section.

Note

The recommended Firewall settings are **Allow HTTPS access through the firewall**, and **Allow SSH access through the firewall**. All other settings should be used in conjunction with Trusted Hosts Settings.

4. Enter the forwarding rules that will apply to packets being forwarded to systems that run behind the firewall.
5. Click **Submit**. A message indicates that service will be interrupted while the new interface is added.
6. Click **OK** to confirm.

To change the HTTP port used by the system:

1. Enter a new HTTP port for the system to use in the **Set HTTP access port** field.
2. Click the **Submit** button.

Note

Be sure to connect to the system using the new configured HTTP port.

© 2014 Edgewater Networks, Inc. All rights reserved.

To enable the firewall logging function:

1. Enable or disable firewall logging by clicking the **Enable Firewall Logging** checkbox.
2. Click the **Submit** button.



Caution

Logging WAN traffic creates a large number of system log messages and affects the system's performance.

Enabling HTTPS Access

To access the system from the WAN or public interface, you need to enable HTTPS access on the **Firewall** page. Access from the LAN or private interface using HTTPS is NOT enabled by default on certain platforms types. To verify your requirements, view the help link on the **Firewall** page.

When you enable HTTPS access, you need to configure an HTTPS certificate. See Configuring an HTTPS Certificate for more details.

Defining Trusted Hosts

Define a list of hosts or networks that are allowed to access the system via the management protocols specified in the **Firewall** page. Refer to Configuring Firewall Settings. The basic firewall rules will be applied only to the listed addresses. All other addresses will be blocked from accessing the device.



The first IP address/Network Address that you add should be the IP address/subnet that includes the IP address of your computer. Otherwise, you will be locked out of the EdgeMarc.

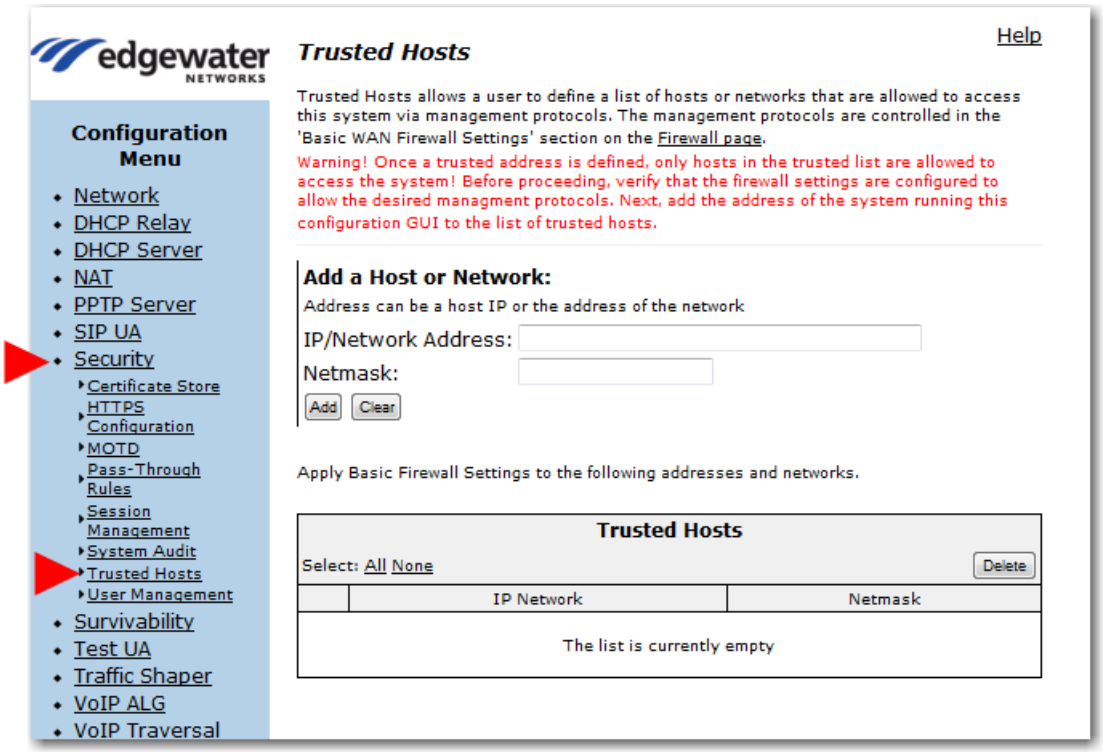
For example, to include the whole LAN side of the network, add the following addresses:

IP/Network Address = 192.168.1.0

Netmask = 255.255.255.0

1. Select **Security > Trusted Hosts** from the Configuration Menu.

© 2014 Edgewater Networks, Inc. All rights reserved.



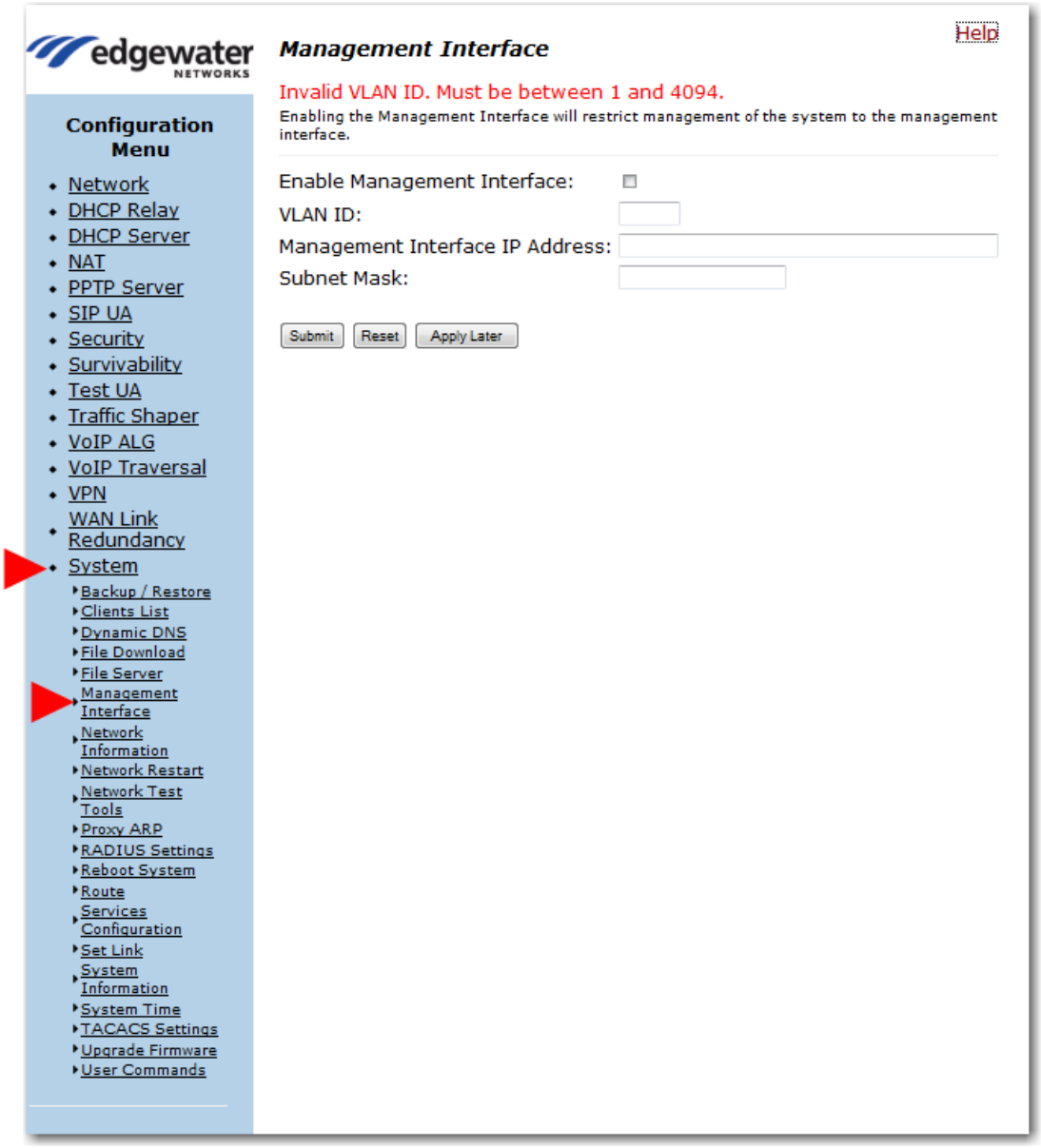
2. Enter the IP address or network address of the subnet to be managed.
3. Enter the Netmask to apply to the IP/Network Address. The Netmask determines how many addresses will be available in the network.
4. Press **Submit**.

Restricting Access to the Management Interface

You can restrict which management protocols such as HTTPS, SSH, SNMP, TELNET are allowed to access the EdgeMarc through the management port. When enabled, ONLY connections from management protocols such as HTTP, SSH, SNMP, TELNET will be allowed on the management port. Access to HTTP, SSH, SNMP or Telnet on WAN or LAN interfaces will be denied.

To enable this feature, select **System > Management Interface** from the **Configuration Menu** and configure the following settings.

© 2014 Edgewater Networks, Inc. All rights reserved.



1. Click the checkbox next to **Enable Management Interface**.
2. On certain systems, the management interface is a tagged VLAN off of the WAN interface. Enter the tagged VLAN ID here. The VLAN ID must be between 1 and 4094.
3. Enter a valid IP address assigned to the Management Interface.

Note
This IP address MUST be on a different subnet than the WAN or LAN interfaces.

4. Enter the Subnet mask for the Management Interface IP address.
5. Click **Submit**.

© 2014 Edgewater Networks, Inc. All rights reserved.

Configuring an HTTPS Certificate

If you enabled HTTPS on the **Firewall** page, you need to configure the device certificate used by HTTPS for secure remote management. The Certificate Store contains certificates for use with HTTPS and/or VoIP Traversal. All certificates are kept in the Certificate list and can be downloaded from there.

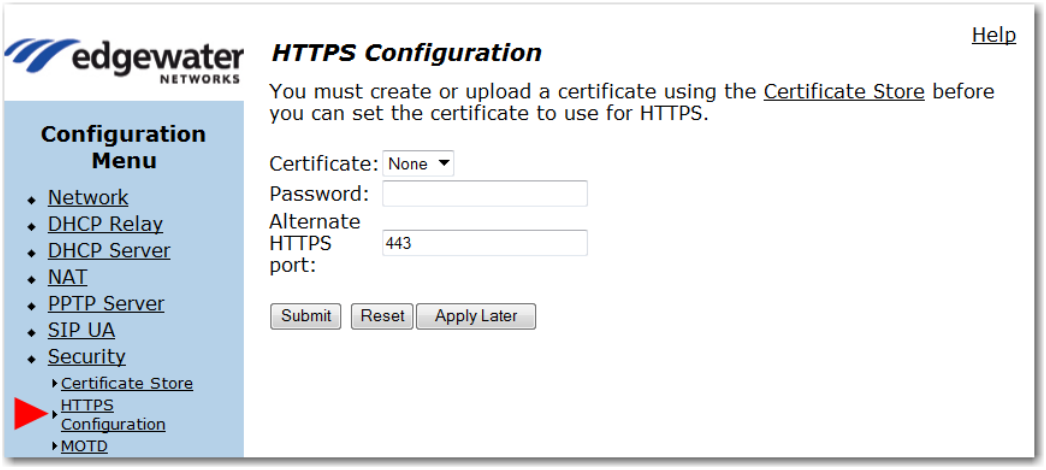
Note

You must create or upload a certificate on the **System > Certificate Store HTTPS** page before you can set the certificate for use with HTTPS. See the online help for the **Certificate Store HTTPS** page for more details.

The **HTTPS Configuration** page allows you to configure the certificate used by HTTPS for secure remote management as well as any alternate HTTPS port to use.

To configure an HTTPS Certificate:

1. Open the **Security > HTTPS Configuration** page from the Configuration Menu.



2. Select the certificate to be used for HTTPS-based device authentication from the **Certificate** drop down box. The certificates that were created and uploaded on the **Security > Certificate Store** page are listed here.
3. (Optional) Enter the password that protects the private key file.
4. Enter an Alternate HTTPS port number. This is the port number that the system's web server will use to listen for inbound management HTTPS requests. By default this port is 443. If you change this port and you currently use port 443 to connect to the web configuration GUI to make this change, you will need to change your browser URL to https:// [ip-of-device] : [alternate-https-port] after you submit this page.

Deploying the EdgeMarc

For details about how to configure and deploy the EdgeMarc appliance in your network, refer to the EdgeMarc online help and the *Edgewater Networks VOS for EdgeMarc User Manual*.

© 2014 Edgewater Networks, Inc. All rights reserved.

The EdgeMarc can be deployed as a Session Border Controller in a network. It can also be deployed in a network behind an existing firewall. For more information about deploying your EdgeMarc behind a firewall, visit our support knowledgebase at www.edgewaternetworks.com/kb.

© 2014 Edgewater Networks, Inc. All rights reserved.