

SANGFOR CMC 5.0


for NGAF User Manual



Declaration

Copyright © SANGFOR Technologies Co., Ltd. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Co., Ltd.

SANGFOR, SINFOR and  logo are the trademarks of SANGFOR Technologies Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

The information in this document is subject to change without notice.

To obtain the latest version, contact the international service center of SANGFOR Technologies Co., Ltd.

About This Document

Organization

- Part I Introduces the installation guide to the CMC product of SANGFOR. This part describes the appearance, functions, and performance specifications of the CMC equipment, and preparations and precautions for its connection.
- Part II Introduces how to use and log in to the CMC console.
- Part III Introduces the deployment of the CMC and NGAF equipments.
- Part IV Introduces the functions and configurations of the CMC Web Console.
- Part V Describe how to connect with other products with CMC.



This document takes SANGFOR CMC5100 as an example. Equipment of different models differs in both hardware and software specifications. Therefore, confirm with SANGFOR about problems involving product specifications.

Conventions

GUI Conventions

Item	Sign	Example
Button	Frame+shadow+shading	The OK button can be simplified as OK .
Menu item	{ }	The menu item System Setup can be simplified as System Setup .
Choose cascading menu items	→	Choose System Setup > Interface Configuration .
Drop-down list, option button, check box	[]	The Enable User check box can be simplified as Enable User .

Window name	Bold Font	Open the New User window.
Prompt	“”	The prompt “Succeed in saving configuration. The configuration is modified. You need to restart the DLAN service for the modification to take effect. Restart the service now?” is displayed.

Symbol Conventions

The symbols that may be found in this document are defined as follows:



Caution: alerts you to a precaution to be observed during operation. Improper operation may cause setting validation failure, data loss, or equipment damage.



Warning: alerts you to pay attention to the provided information. Improper operation may cause bodily injuries.



Note or tip: provides additional information or a tip to operations.

Technical Support

Email: tech.support@sangfor.com.hk

International Service Centre: +60 12711 7129 (7511)

Malaysia: 1700817071

Website: www.sangfor.com

Acknowledgement

Thanks for choosing our product and user manual. For any suggestions on our product or user manual, provide your feedback to us by phone or email.

Table of Content

Declaration	i
About This Document	ii
Organization	ii
Conventions	ii
GUI Conventions	ii
Symbol Conventions	iii
Technical Support	iii
Acknowledgement	iii
Table of Content	iv
 Chapter 1 Installation Guide	 1
1.1. Environment Specifications	1
1.2. Power Supply	1
1.3. Appearance	1
1.4. Configuration and Management	2
1.5. Equipment Connection	2
Chapter 2 Introduction to the Console	4
2.1. Logging In to the Web UI	4
Chapter 3 CMC and NGAF Deployment	6
3.1. CMC Device Deployment Modes	7
3.1.1. Gateway Mode	7
3.1.2. Single-arm mode	8
3.2. NGAF Deployment	9
3.2.1. NGAF as Gateway Mode	9
3.2.2. NGAF as Transparent mode	9
3.2.3. NGAF in VRRP environment	12
3.2.4. NGAF as Mirror mode	13
Chapter 4 CMC Web Console	14
4.1. Status	14
4.1.1. CMC Status	14
4.1.2. Site Monitoring	16
4.1.3. NGAF Site Summary	26
4.1.4. Auto Update Status	31
4.1.5. Services	32
4.1.6. Logs	34
4.1.7. Config Distribution Status	38
4.2. Site Management	38
4.2.1. Groups/Sites	38
4.2.2. TCP Proxy	61
4.2.3. Schedule Tasks	63
4.2.4. Update Packages	67
4.2.5. Central Management	68
4.3. System	68
4.3.1. Basics	68




4.3.2. Network.....	71
4.3.3. NGAF Central Mgt	76
4.3.4. Administrators	79
4.3.5. Database Management	87
4.3.6. Advanced.....	88
4.3.7. Firewall	91
4.3.8. Backup/Restore	96
4.3.9. Email Alarm Options.....	96
4.3.10. Email Alarm Service	98
4.3.11. Auto-Update Server.....	99
4.3.12. Time Deviation Reminder	100
Chapter 5 Sites Connecting.....	102
5.1. Creating Sites	102
5.2. Connecting to the CMC	106
5.3. Common Causes for Config Distribution Failure	110

Chapter 1 Installation Guide

This part describes the composition and hardware installation of the CMC series products of SANGFOR. You can configure and commission the product after the hardware is correctly installed.

1.1. Environment Specifications

The environment specifications of the SANGFOR CMC equipment are listed as follows:

-  Input voltage: 110-230 V
-  Temperature: 0-45°C
-  Humidity: 5%-90%

Take proper grounding and dustproof measures, and keep good ventilation and stable room temperature in the application environment to ensure long-term and stable operation of the system.

The product complies with the design requirements in terms of environment protection. The deployment, application, and scrapping of the product must be in accordance with national laws and regulations.

1.2. Power Supply

The SANGFOR CMC series products are supplied with 110-230 V AC power. Before connecting power to the product, ensure that proper grounding measures are taken for the power supply.

1.3. Appearance



Figure 1 Front panel (CMC M5100)

1. CONSOLE interface
2. USB
3. MANAGE interface
4. ETH3
5. ETH2
6. ETH1



The ALARM indicator is steady on in red during startup of the equipment. If the indicator turns off after 1-2 minutes, the equipment is started properly. If the indicator does not turn off for a long period of time, power off the equipment and then start it again after 5 minutes. If the problem persists, contact the customer service center to confirm whether the equipment is damaged. After the equipment is started properly, the ALARM indicator may blink in red sometimes. This means that the equipment is writing system logs.



The CONSOLE interface is used only for development and commissioning. End users connect to the equipment through the CONSOLE interface.

1.4. Configuration and Management

Before configuring the equipment, get a computer ready and ensure that the webpage browser (such as the Internet Explorer) installed on the computer works properly (Firefox, Opera, Safari, Chrome and any non-IE browser are not supported). Then connect the computer to the same local area network (LAN) as the SANGFOR CMC equipment and configure the equipment.

The management interface of the CMC equipment is MANAGE (ETH0) and its default IP address is 11.254.254.254/24. The DMZ interface of the CMC equipment is ETH1 and its default IP address is 10.254.253.254/24. Connect the MANAGE (ETH0) interface to the LAN or directly to the computer by using a network cable at initial login.

1.5. Equipment Connection

Connect the power cable on the backplane and turn on the power switch. Then the POWER indicator (green) and ALARM indicator (red) on the front panel becomes on. The ALARM indicator turns off in 1-2 minutes, which indicates that the gateway works properly.

Connect the MANAGE (ETH0) interface to the LAN by using a network cable with an RJ-45 connector and then configure the CMC equipment.

After logging in to the console, perform network connection and connect cables based on the network environment and deployment requirements.



Multi-line SC device can support multiple ISP lease lines. In this case, connect the second ISP line to the WAN2 interface, the third ISP line to WAN3 interface and so on.



When the equipment works properly, the POWER and LINK indicators are steady on. The ACT indicator blinks in case of data flows. The ALARM indicator (red) is on for about 1 minute at startup due to system loading, and is off in normal operation. If the ALARM indicator is steady on during installation, power off the equipment and then start it again. If the problem persists, contact SANGFOR.



Use a straight-through cable to connect the network interface directly to a modem or switch, and a crossover cable to connect network interface to a router. If the indicators are normal but the cable connection fails, check whether a wrong network cable is used. A straight-through cable differs from a cross-over cable in the wire sequence at both ends. See the figure below.

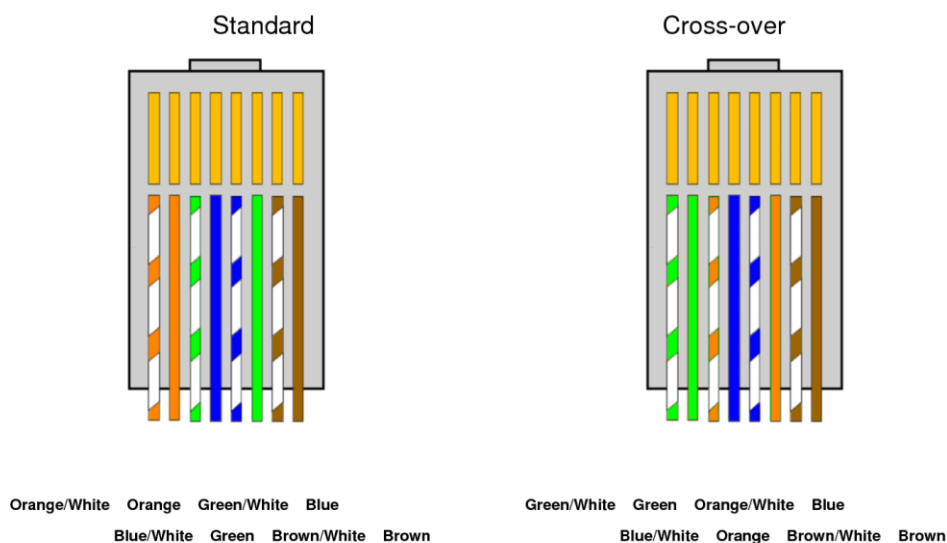


Figure 2 Wire sequences of straight-through cables and cross-over cables

Chapter 2 Introduction to the Console

2.1. Logging In to the Web UI

The CMCEquipment supports Hypertext Transfer Protocol Secure (HTTPS) login through a standard HTTPS port. If you log in through the MANAGE interface at initial login, the URL is <https://11.254.254.254>.

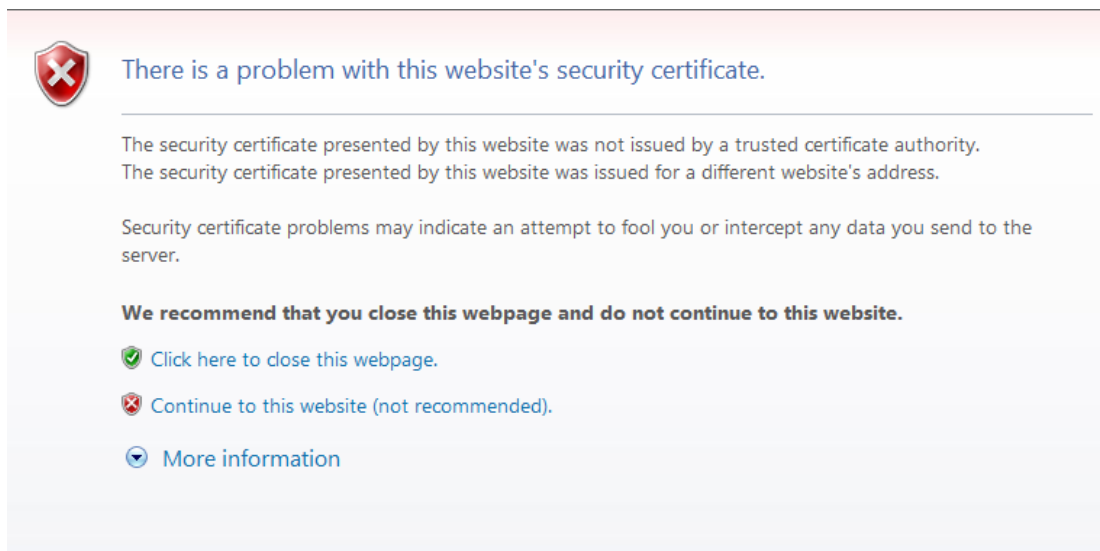


Login to the Web UI of the CMC equipment through HTTPS can avoid security threats caused if the configurations are intercepted during transmission.

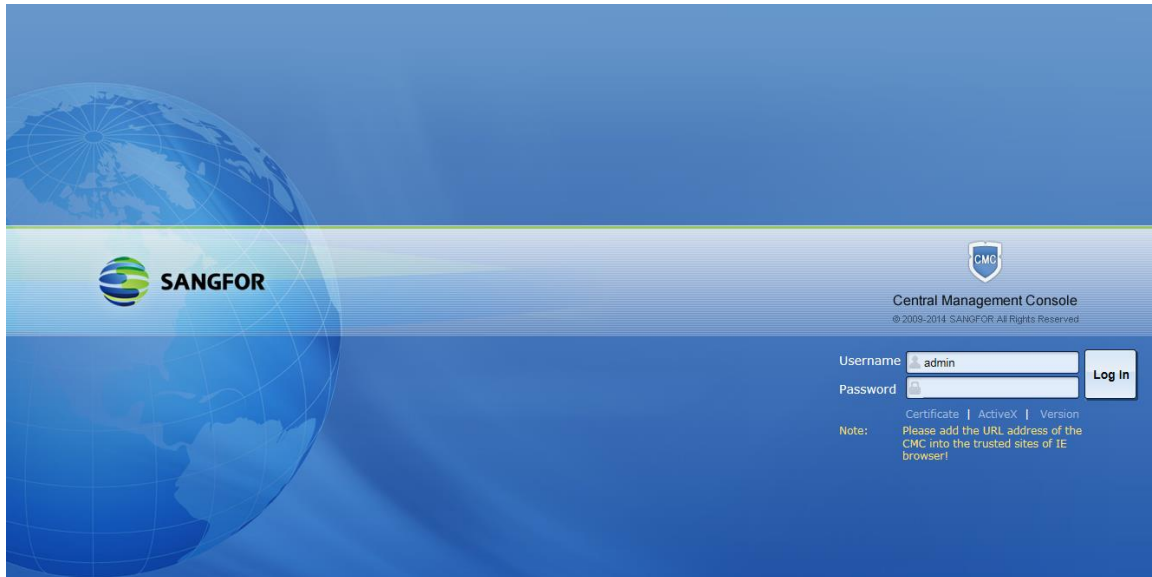
How to log in to the console page of the CMC equipment?

Connect the cables as described earlier and then configure the CMC equipment on the Web UI. The procedure is as follows:

Configure an IP address (11.254.254.100 for example) on the 11.254.254.X network segment for the computer from which you log in to the console. Then enter the default login IP address and port number of the MANAGE interface on the address bar of the Internet Explorer, that is, <https://11.254.254.254>. A safety prompt shown in the figure below is displayed.



Click **Yes** and the login interface shown in the figure below is displayed.



Enter the user name and password and click **Log In**. the default user name and password are both **admin**.

To view the version of the current gateway, click **Version**.

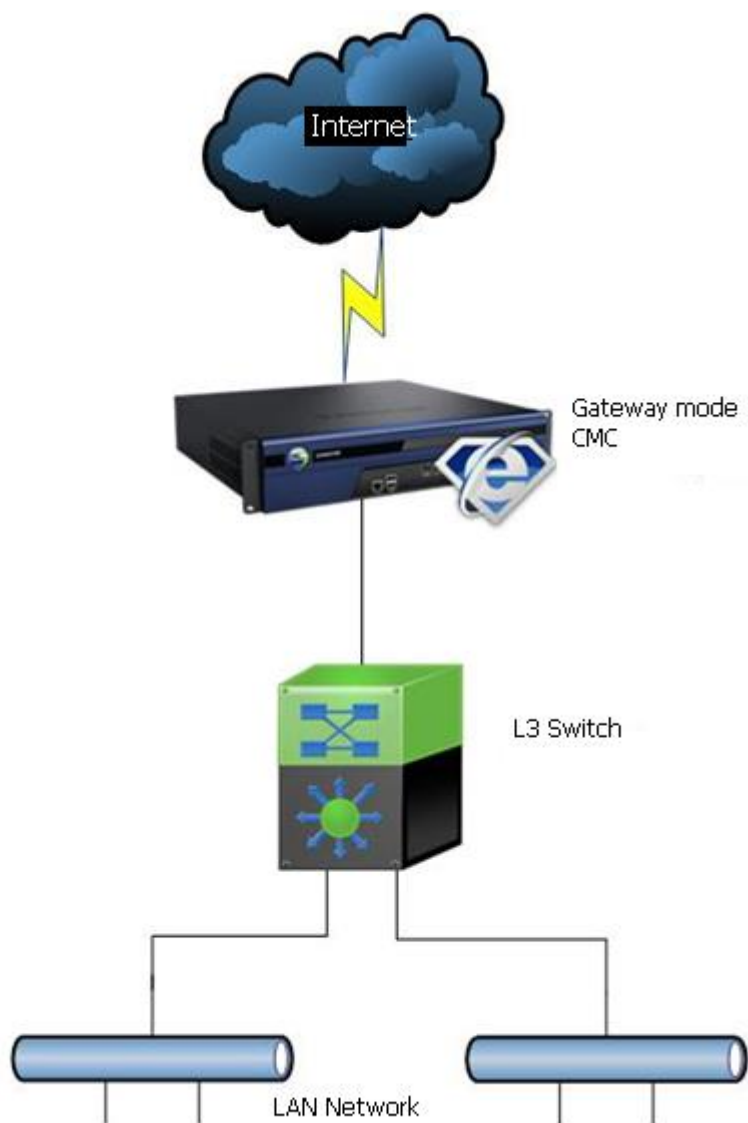
You do not need to install any control for logging in to the console. You can log in to the console by using another browser instead of the Internet Explorer.

Chapter 3 CMC and NGAF Deployment

This chapter introduce Sangfor CMC deployment methods.

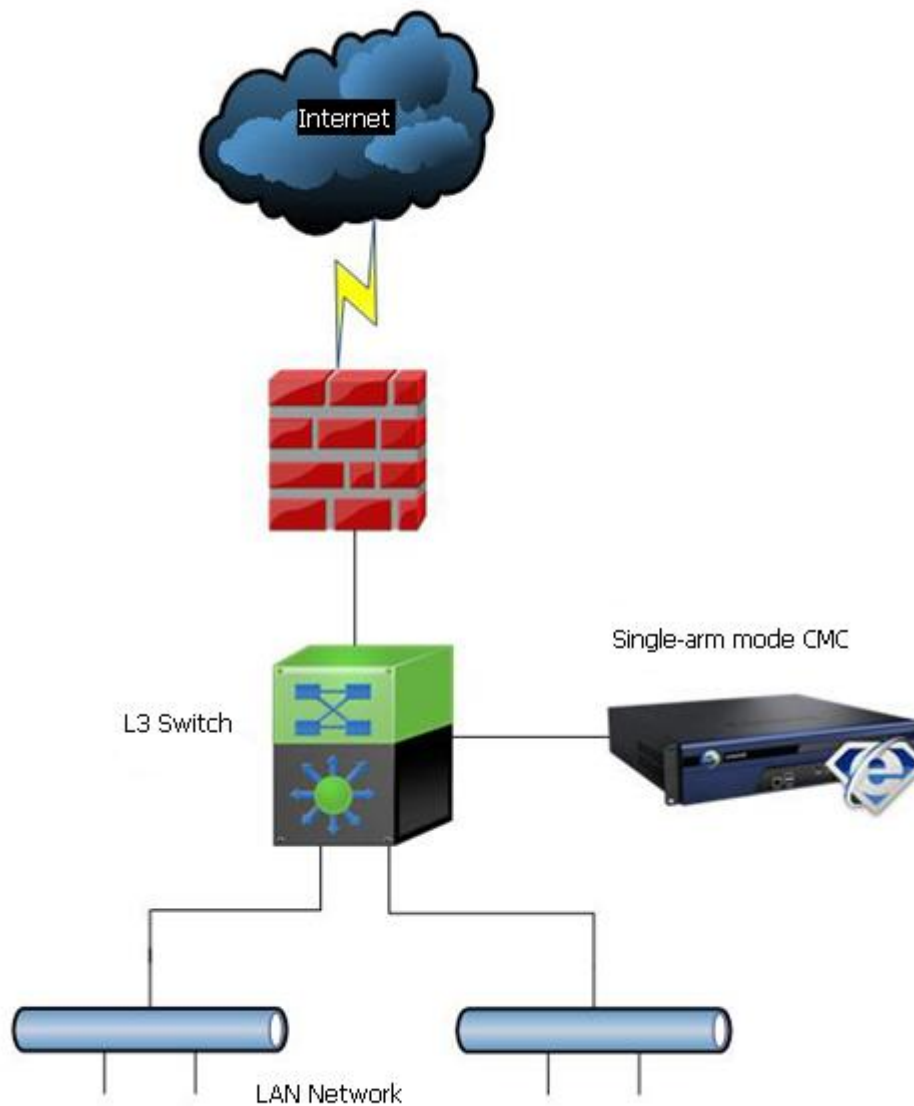
3.1. CMC Device Deployment Modes

3.1.1. Gateway Mode



CMC device in gateway deployment mode, WAN interface can connect to public network and LAN interface connects to LAN network directly without port mapping needed. Meanwhile, NGAF can get authenticated and download configuration in CMC via port 5000 by default.

3.1.2. Single-arm mode



CMC deployed in single-arm mode, LAN interface connects to core-switch LAN port and port-mapping needed to be done at gateway device (such as firewall, router and etc). Ports needed are:

TCP ports : 5000, 443, 1500, 446, 5109, 9458

UDP ports : 5000

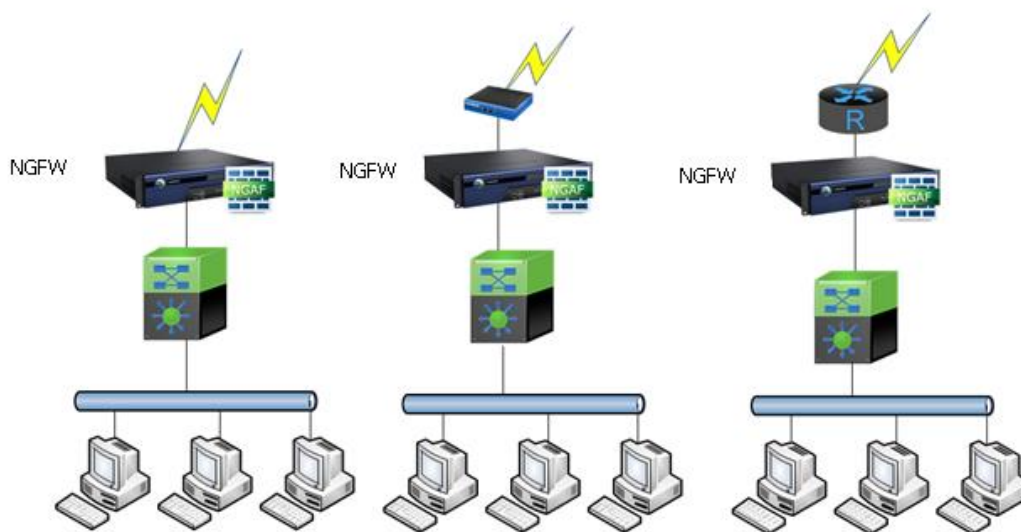


Single-arm deployment mode of CMC is recommended.

3.2. NGAF Deployment

3.2.1. NGAF as Gateway Mode

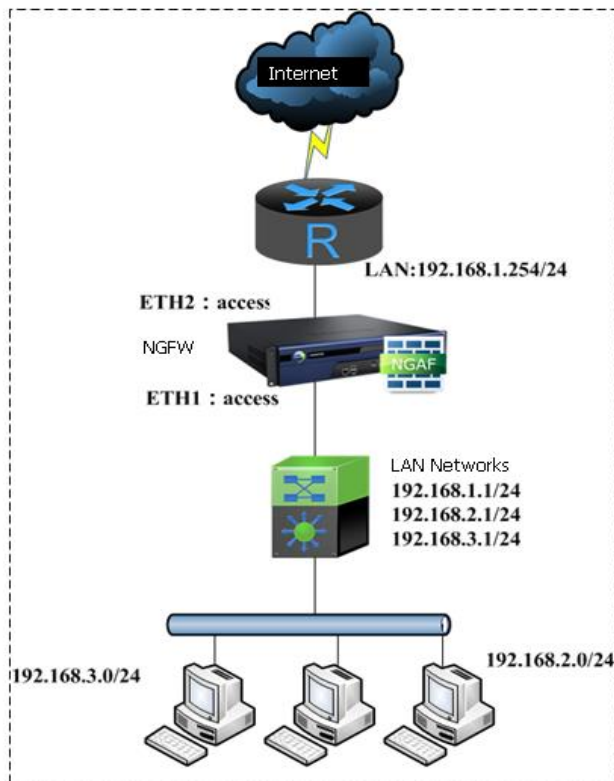
Gateway mode NGAF device is deployed in the public network as router which can proxy for internal user to access Internet as shown below:



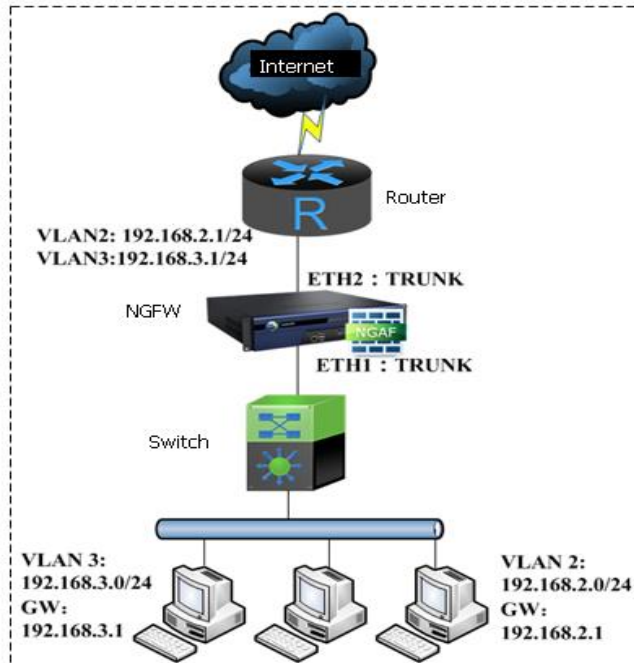
3.2.2. NGAF as Transparent mode

NGAF transparent deployment mode supports **ACCESS port** connection and **TRUNK port** connection.

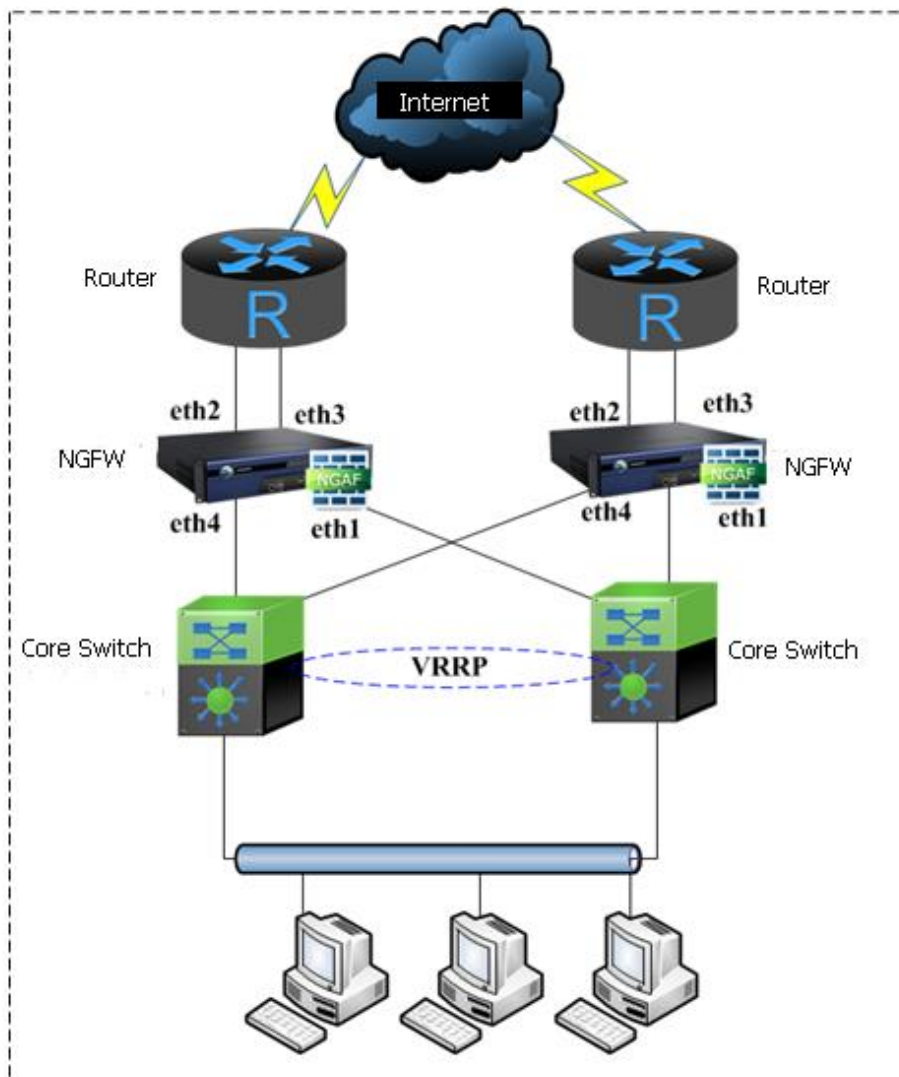
By referring to the topology below, NGAF deployed as transparent mode, LAN interface is connected to a L3 switch with two network segments 192.168.2.0/255.255.255.0 and 192.168.3.0/255.255.255.0. NGAF connected as ACCESS port.



Transparent deployment mode NGAF; core switch ports assigned VLAN segments but routing feature is not enabled; Router as gateway for all VLAN networks. LAN networks includes 192.168.2.0/255.255.255.0 and 192.168.3.0/255.255.255.0 which belongs VLAN2 and VLAN3 accordingly, trunking protocol is used between core-switch and router.

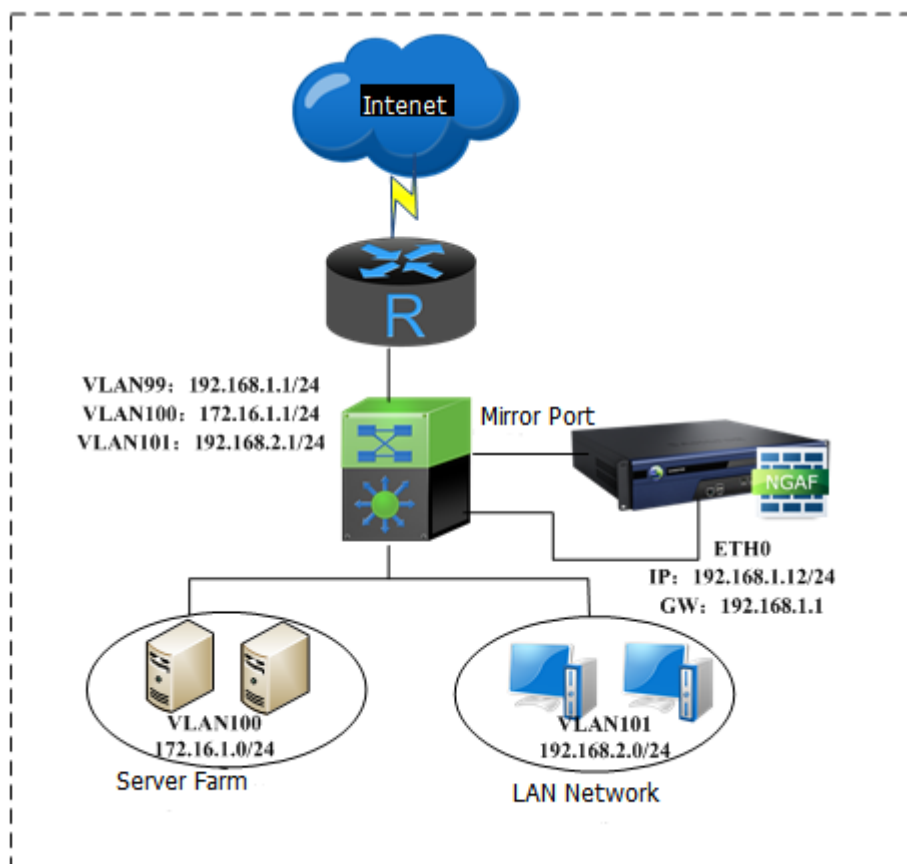


3.2.3. NGAF in VRRP environment



If customer's network topology is similar with the figure above; there are two layer 3 core switches and two routers performing load balancing, NGAFs are deployed as transparent mode to prevent changes happen in the network.

3.2.4. NGAF as Mirror mode



Bypass mode can enable protection at the same time can maintain customer's network environment and prevent the risk of user's network disruption. Connect the NGAF device with switch's mirror port or HUB and ensure that the user traffics forward to servers pass by the switch or HUB, then enable mirroring download and upload traffics during configuration for mirror port and enable server protection.

The network topology above shows NGAF device deployed as bypass mode, LAN interface connects to layer 3 switch, the network segment is 192.168.2.0/24, server farm network segment is 172.16.1.0/24. Customer's requirement is NGAF can perform IPS, WEB application protections and DLP protection.

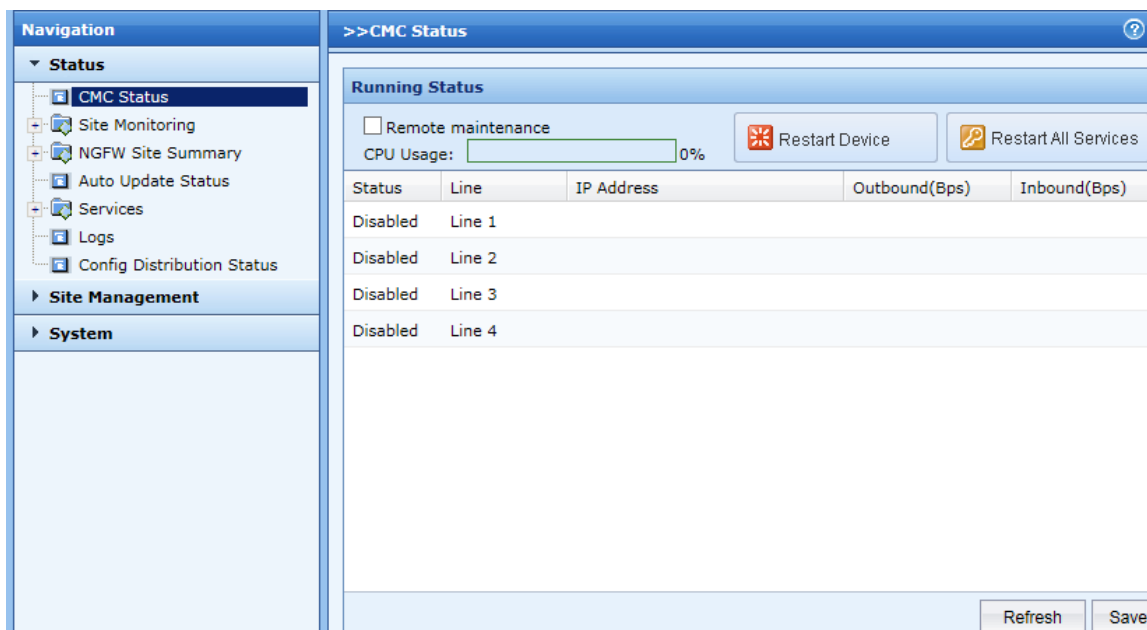
Chapter 4 CMC Web Console

4.1. Status

This section include [CMC status], [Site Monitoring], [NGAF Site Summary],[Auto Update Status], [Services],[Logs] and [Config Distribution Status] modules.

4.1.1. CMC Status

[CMC Status] include [CPU Usage], [Extranet Interface Line Status], [IP address], [Outbound Traffics] and [Inbound Traffics], [Remote Maintenance], [Restart Device] and [Restart All Services] function modules as shown below:



Status	Line	IP Address	Outbound(Bps)	Inbound(Bps)
Disabled	Line 1			
Disabled	Line 2			
Disabled	Line 3			
Disabled	Line 4			

[CPU Usage] : Display real time CPU usage of CMC device.

[Remote maintenance] : Check this option to allow Webconsole access through WAN interface.

[Restart Device] : Click the button to reboot hardware of the CMC device.

[Restart All Services] : Click the button to restart all services running in CMC device but not



SANGFOR Technologies Inc.

International Service Centre: +60 12711 7129 (7511)

Malaysia: 1700817071

Email: tech.support@sangfor.com

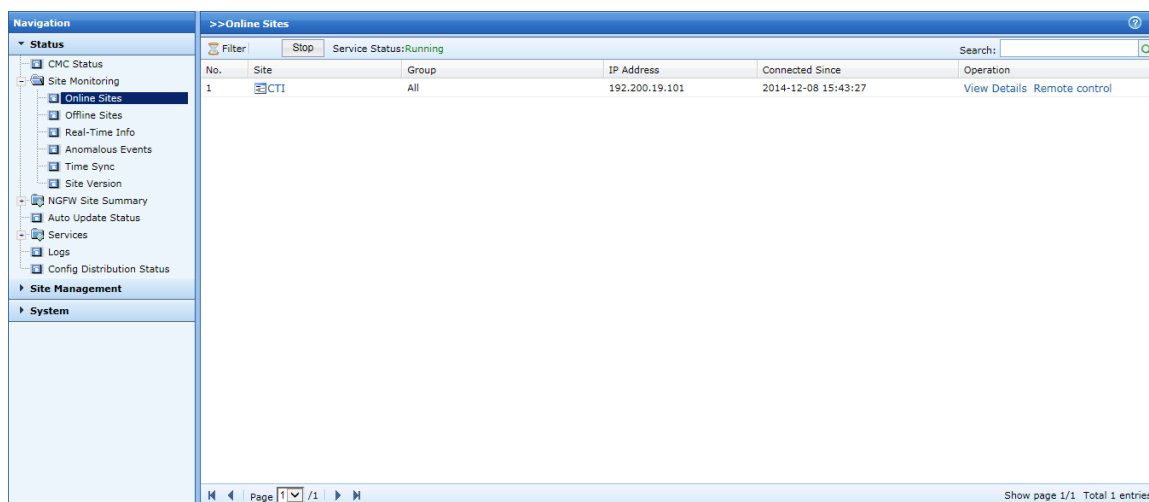
hardware reboot.

4.1.2. Site Monitoring

[Site Monitoring] includes [Online Sites], [Offline Sites], [Real-Time Infor], [Anomalous Events], [Time Sync] and [Site Version] modules.

4.1.2.1 Online Sites

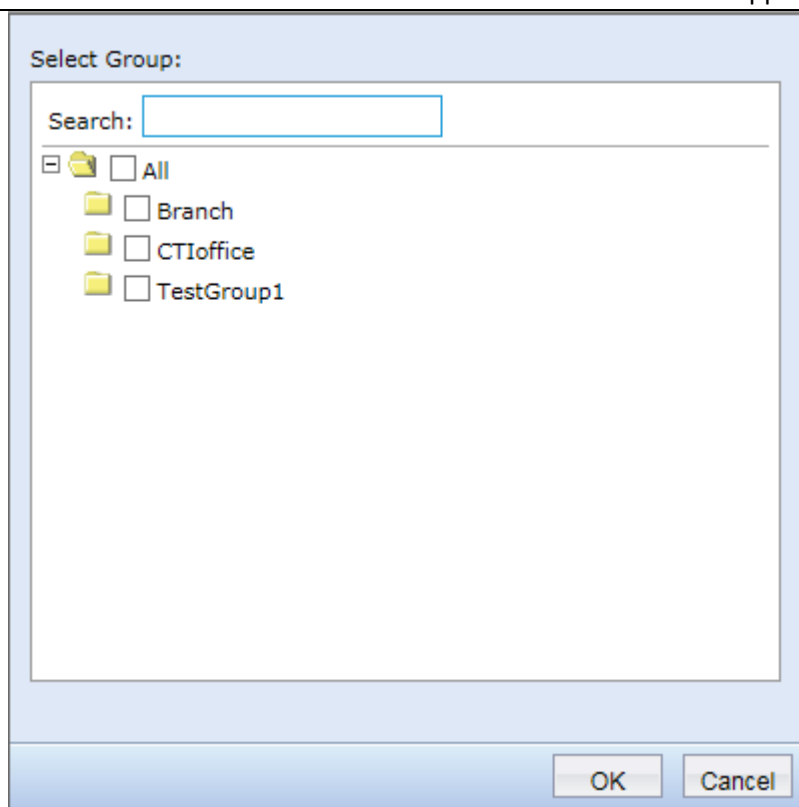
[Online Sites] includes [Stop services], [Filter] and [Search] function module. This page also display all online Sites, IP address, Connected time and operations such as View, Details and Remote control as shown in the figure below:



No.	Site	Group	IP Address	Connected Since	Operation
1	CTI	All	192.200.19.101	2014-12-08 15:43:27	View Details Remote control

[Stop] : Click on the button and all CMC services will be stopped, all connected sites will be dropped.

[Filter] : [Filter] : Use the filter feature when there are many sites in order to narrow down the sites resulted by using selected parameters. Click on the button and the following figure is shown:



Select the related group and click **OK**.

[Search] : Insert related group/sites name and click on **Search**, the search results will be displayed.
Support fuzzy search but does not support wildcard search.

[View Details] : Click on the button to check on the details between CMC and sites as shown below:

Total Speed: 0 Bps (Outbound: 0 Bps; Inbound: 0 Bps)		
Channel Name	Speed(Out Bps/In Bps)	Line Selection Details
Command channel	0 / 0	[0]192.200.19.107<->[0]192.200.19.101
File channel	0 / 0	[0]192.200.19.107<->[0]192.200.19.101
Real-time info channel	0 / 0	[0]192.200.19.107<->[0]192.200.19.101
<div>Close</div>		

[Command Channel] : Channel used to transfer commands between CMC and NGAF, all command traffics will be forwarded via this channel.

[File Channel] : Use to transfer configurations traffics with NGAF during auto/manual distributing configuration.

[Real-time info channel] : Channel for CMC and NGAF to send information, such as real time status of NGAF is forwarded via this channel.

Click on **Close** to close the page.

[Remote Control] : Click on the botton to control the NGAF via TCP proxy method as shown below:

Prompt: **Right Checking Successful**

Note:

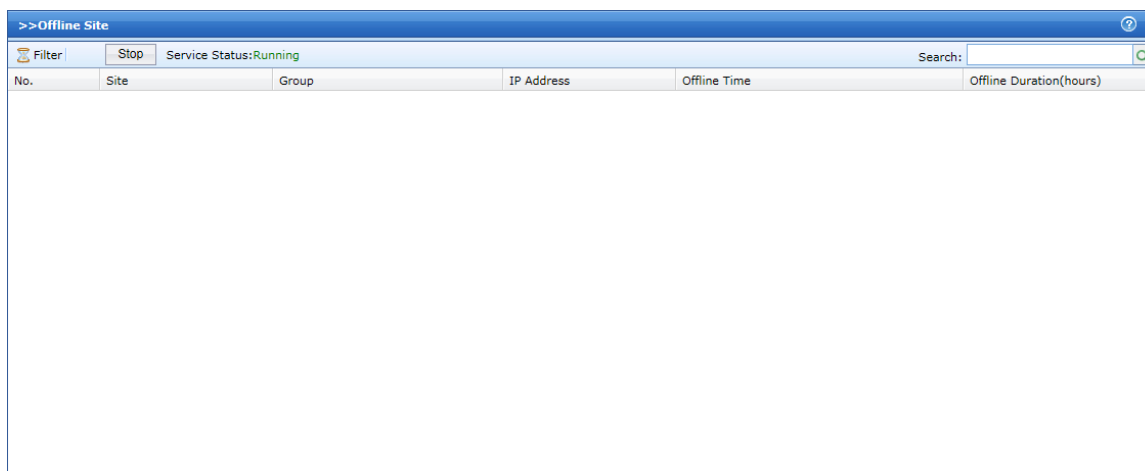
1. If the page fails to display normally, please download ActiveX and add the URL address of the CMC into trusted sites on your browser.
2. Closing this page will disconnect your remote access session.

Service	IP Address	Port	Description	Status
Console	127.0.0.1	20794	Default service	Listening
Data Center	127.0.0.1	22080	Default service	Listening
RealTime Log	127.0.0.1	21188	Default service	Listening

Refer to section 4.2.3 for TCP proxy service details.

4.1.2.2 Offline Sites

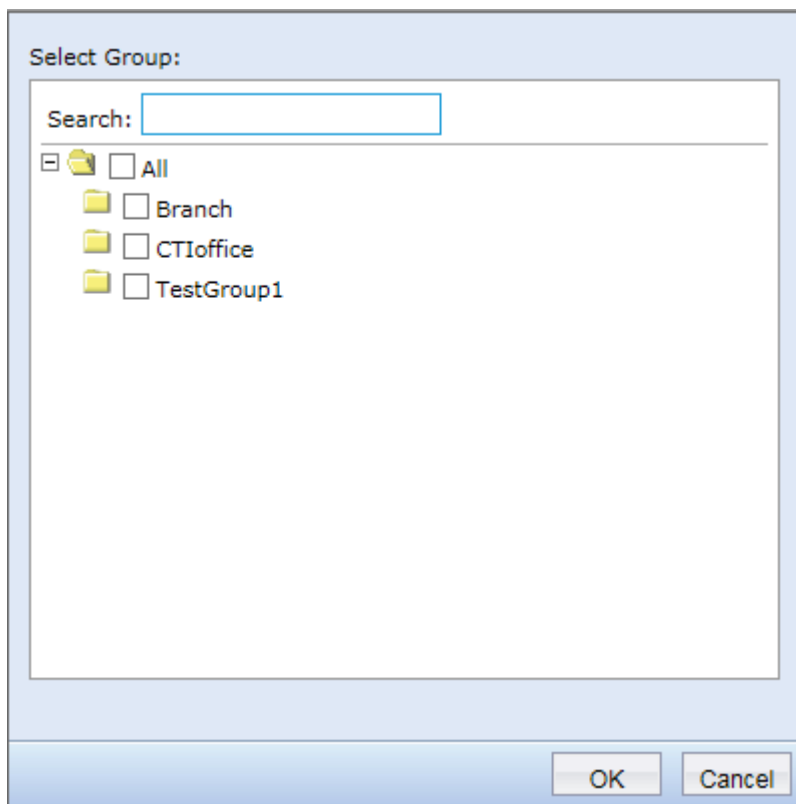
[Offline Sites] includes [Stop Service], [Filter] and [Search] function module. This page also display all offline sites name, IP address, offline time and offline duration messages as in the following:



No.	Site	Group	IP Address	Offline Time	Offline Duration(hours)
-----	------	-------	------------	--------------	-------------------------

[Stop] : Click on the button and all CMC services will be stopped, all connected sites will be dropped.

[Filter] : Use the filter feature when there are many sites in order to narrow down the sites resulted by using selected parameters. Click on the button and the following figure is shown:



Select the related group and click **OK**.

[Search] : Insert related group/sites name and click on **Search**, the search results will be displayed. Support fuzzy search but does not support wildcard search.

4.1.2.3 Real-Time Info

[Real-Time Info] includes [Stop] service, [Filter] and [Search] functions. This page displays all current connected NGAF status, CPU usage, hard disk usage, Memory(RAM) usage, WAN inbound/outbound traffics flow and VPN tunnel inbound/outbound traffics flow information. The page is shown below:

>>Real-time Info

Filter: [Stop] Service Status: Running Search: []

Site	Status	Resource Usage(%)			WAN Speed(Bps)		VPN Tunnel Speed(Bps)		VPN Tunnels
		CPU	Disk	Memory	Outbound	Inbound	Outbound	Inbound	
CTI	Online	8	2	22	0	0	-	-	-

[Stop] : Click on the button and all CMC services will be stopped, all connected sites will be dropped.

[Filter] : Use the filter feature when there are many sites in order to narrow down the sites resulted by using selected parameters. Click on the button and the following figure is shown:

Site Status: ☒ Online ☒ Offline

Select Group/Site:

Search: []

- ☒ All
- ☒ Branch
- ☒ CTIOffice
- ☒ TestGroup1

OK Cancel

[Site Status] : Include online and offline status, can view which are the sites online and which are offline. For example: if there are online and offline NGAF in group/sites, when both online and offline options are selected, online NGAF real time information is shown meanwhile for offline NGAF shows

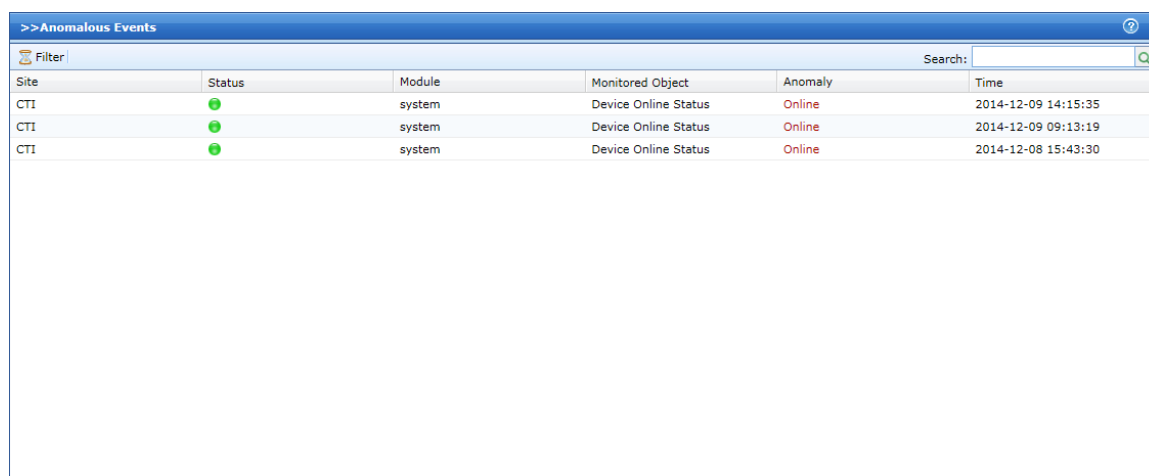
only device name without other information.

[Select Group/Site] : Choose the related group/site and click **OK** to get expected results.

[Search] : Insert related group/sites name and click on **Search**, the related device's real time information will be displayed. Support fuzzy search but does not support wildcard search.

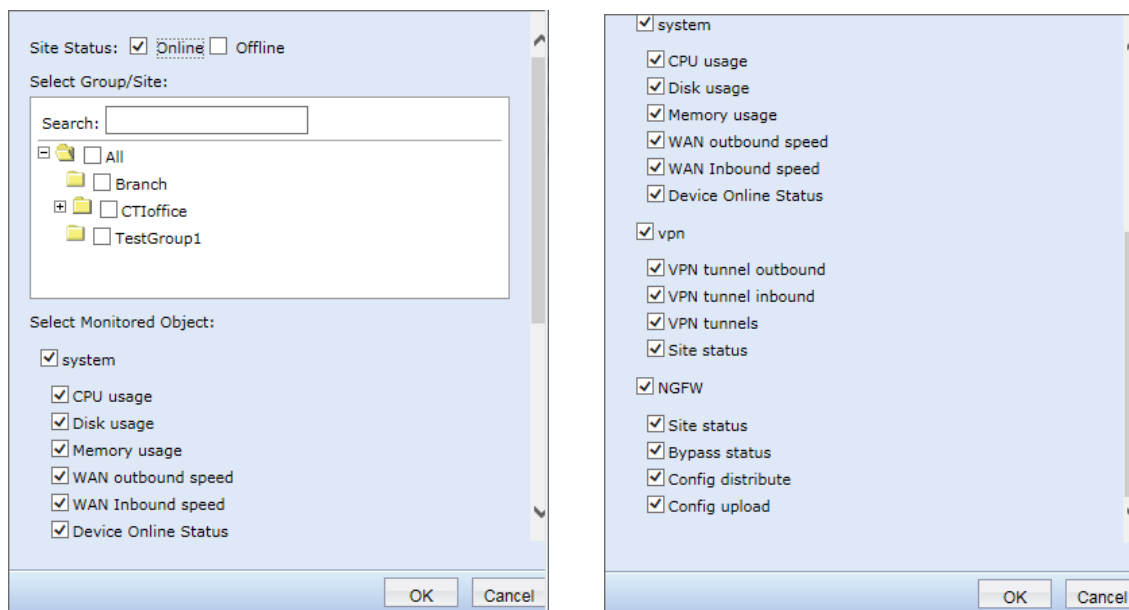
4.1.2.4 Anomalous Events

[Anomalous Events] includes [Filter] and [Search] function modules. This page display all site's anomalous message such as CPU usage 100%, memory usage 100% and etc as shown below:



Site	Status	Module	Monitored Object	Anomaly	Time
CTI	●	system	Device Online Status	Online	2014-12-09 14:15:35
CTI	●	system	Device Online Status	Online	2014-12-09 09:13:19
CTI	●	system	Device Online Status	Online	2014-12-08 15:43:30

[Filter] : Use the filter feature when there are many sites in order to narrow down the sites resulted by using selected parameters. Click on the button and the following figure is shown:



Site Status: ☒ Online ☐ Offline

Select Group/Site:

Search:

☐ All

☐ Branch

☒ CTIOffice

☐ TestGroup1

Select Monitored Object:

☒ system

☒ CPU usage

☒ Disk usage

☒ Memory usage

☒ WAN outbound speed

☒ WAN Inbound speed

☒ Device Online Status

OK Cancel

☒ system

☒ CPU usage

☒ Disk usage

☒ Memory usage

☒ WAN outbound speed

☒ WAN Inbound speed

☒ Device Online Status

☒ vpn

☒ VPN tunnel outbound

☒ VPN tunnel inbound

☒ VPN tunnels

☒ Site status

☒ NGFW

☒ Site status

☒ Bypass status

☒ Config distribute

☒ Config upload

OK Cancel

[Site Status] : Include online and offline status, can view which are the sites online and which are offline. For example : if there are online and offline NGAF in group/sites, when both online and offline options are selected, anomalous information of all NGAF devices will be shown.

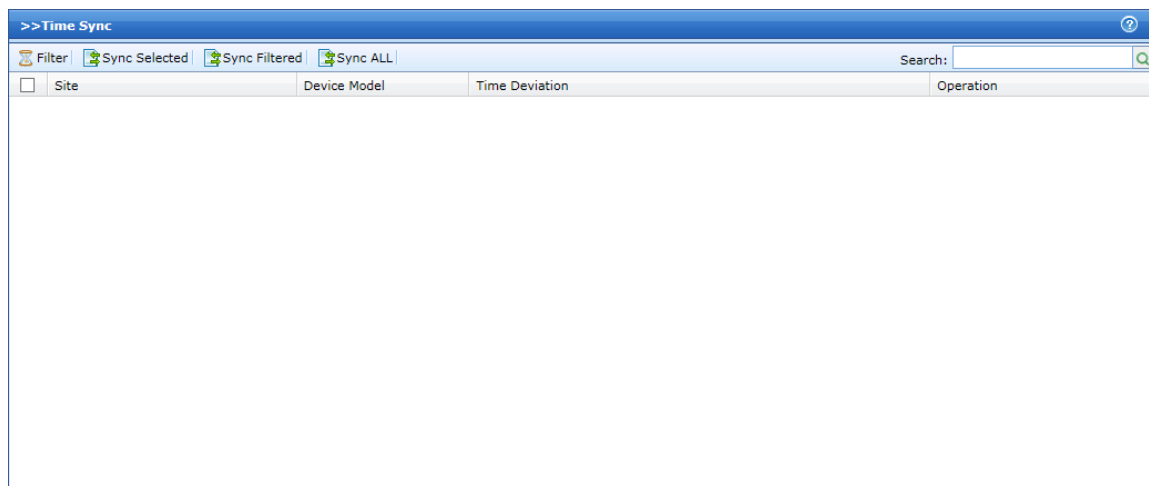
[Select Group/Site] : Choose the related group/site and click **OK** to get expected results.

[Select Monitored Object] :

[Search] : Insert related group/sites name and click on **Search**, the related device's anomalous information will be displayed. Support fuzzy search but does not support wildcard search.

4.1.2.5 Time Sync

[Time Sync] includes [Filter], [Sync Selected], [Sync Filtered], [Sync ALL] and [Search] function modules. This page shows site's time deviation which include also site's name, device's model, time deviation and operation as shown below:



[Filter] : Use the filter feature when there are many sites in order to narrow down the sites resulted which has time deviation with CMC. Click on the button and the following figure is shown:



Model: All

Select Group:

Search:

- ☐ All
- ☐ Branch
- ☐ CTIoffice
- ☐ TestGroup1

OK Cancel

Search and select the related group and site, click on **OK** to get the result.

[Sync Selected] : Select Site and click on the button to synchronize site's system time with CMC system time.

[Sync Filtered] : Use Filter module to get the result sites and click on the button to synchronize filtered sites system time with CMC system time.

[Sync ALL] : Click on the button to synchronize all site's system time with CMC's system time.

[Search] : Insert related group/sites name and click on **Search**, the related sites information will be displayed. Support fuzzy search but does not support wildcard search.



Time deviation is the time difference between site's system time and CMC's system.

4.1.2.6 Site Version

[Site Version] includes [Filter] and [Search] function modules. This page displays the name, module name, current version, update previous version and update time of all sites as shown below:

>>Site Version Info

Filter Search:

Site	Module Name	Current Version	Update Previous Version	Update Time(Time Sync)
CTI	system	4.30.0.0	0.0.0.0	2014-12-08 14:35:00
CTI	CM	4.2.0.0	0.0.0.0	2014-12-08 14:35:00
CTI	vpn	4.32.0.0	0.0.0.0	2014-12-08 14:35:00
CTI	NGFW	5.3.0.0	0.0.0.0	2014-12-08 14:35:00

Page 1 Total 1 Show page 1/1 Total 4 entries

[Filter] : Use the filter feature when there are many sites in order to narrow down the sites resulted by using selected parameters. Click on the button and the following figure is shown:

Select Group:

Search:

☐ All

☐ Branch

☐ CTIOffice

☐ TestGroup1

OK Cancel

Select the related group and click **OK**.

[Search] : Insert related group/sites name and click on **Search**, the search results will be displayed. Support fuzzy search but does not support wildcard search.



Update previous version shown as 0.0.0.0 means site's NGAF related module has not

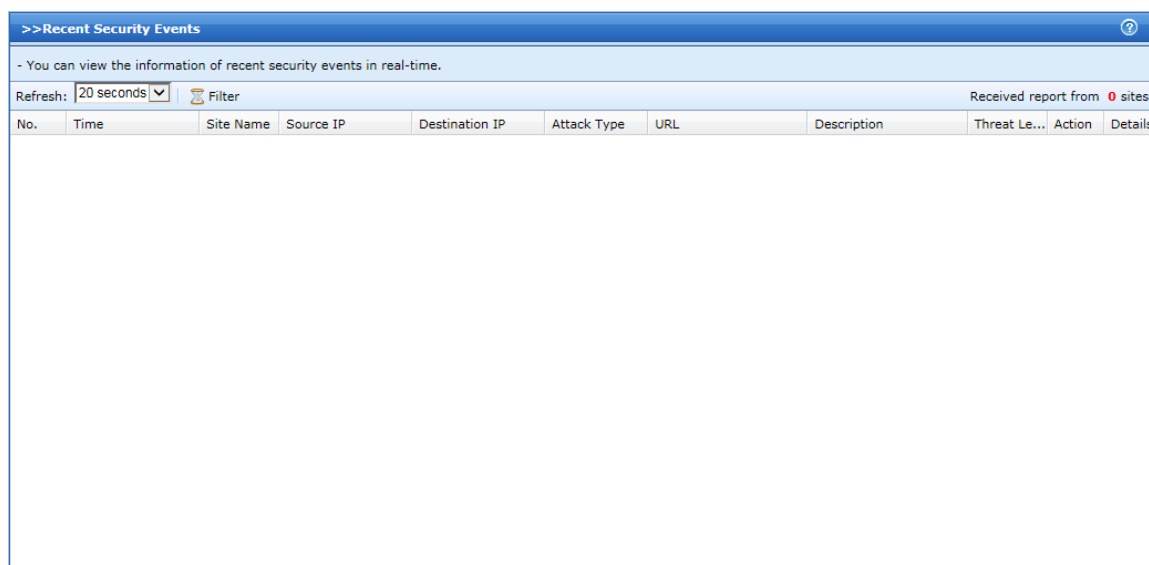
perform auto-update via CMC.

4.1.3. NGAF Site Summary

[NGAF Site Summary] content includes [Recent Security Events], [Security Event Ranking], [App Traffic Tanking] and [Internal database Status].

4.1.3.1 Recent Security Events

[Recent Security Events] includes [Refresh] interval and [Filter] modules. This page displays also NGAF's recent online security events and details which are time, site name, source IP, destination IP, attack type, URL, description, threat level, action and details. The page is shown as below:



No.	Time	Site Name	Source IP	Destination IP	Attack Type	URL	Description	Threat Le...	Action	Details
-----	------	-----------	-----------	----------------	-------------	-----	-------------	--------------	--------	---------

[Refresh] : Configure real time data page refresh period, available options are 10, 20 and 60 seconds.

[Filter] : Select to view security events base on the threat level filtering, selectable options are high, medium and low level.

Event Threat Level

☒ High
☒ Medium
☒ Low

4.1.3.2 Security Events Ranking

[Security Events Ranking] used to show events of NGAF sites which involves DOS attack, web application protection, IPS, virus, APT and attempt count. The page is shown as below:

>>Security Events Ranking of the Week							
View Top: 20		Refresh		Only online sites can connect to the database.			
No.	Site Name	DOS Attack	Web Application Protection	IPS	Virus	APT	Attempt Count
1	CTI	0	0	0	0	0	0
Online							

[View Top] : Display top 10-60 most security events happening sites.

[Refresh] : Refresh the result on display page.

4.1.3.3 App Traffic Ranking

[App Traffic Ranking] includes [View Top] and [Sort] function modules. This page shows Online sites with top traffics flow, application type, outbound, inbound and bidirectional flow speed, percentage and sites details. The page is shown below:

>>App Traffic Ranking						
Refresh: 10 seconds View Top: 10 Sort By: Bidirectional Received report from 1 sites						
No.	App Type	Outbound	Inbound	Bidirectional	Percent	Site Details
1	Funshion	1.8(KB/s)	261.0(B/s)	2.0(KB/s)	86.0%	CTI (2.0 KB/s)
2	HTTP_POST	57.0(B/s)	116.0(B/s)	173.0(B/s)	7.1%	CTI (173.0 B/s)
3	Other	71.0(B/s)	14.0(B/s)	85.0(B/s)	3.5%	CTI (85.0 B/s)
4	Whatsapp Messenger	43.0(B/s)	40.0(B/s)	83.0(B/s)	3.4%	CTI (83.0 B/s)

[View Top] : To show top 10/20/30 traffic flow on the online sites. Refresh the page and the top 10/20/30 applications of each site will be displayed and the previous display will be dumped.

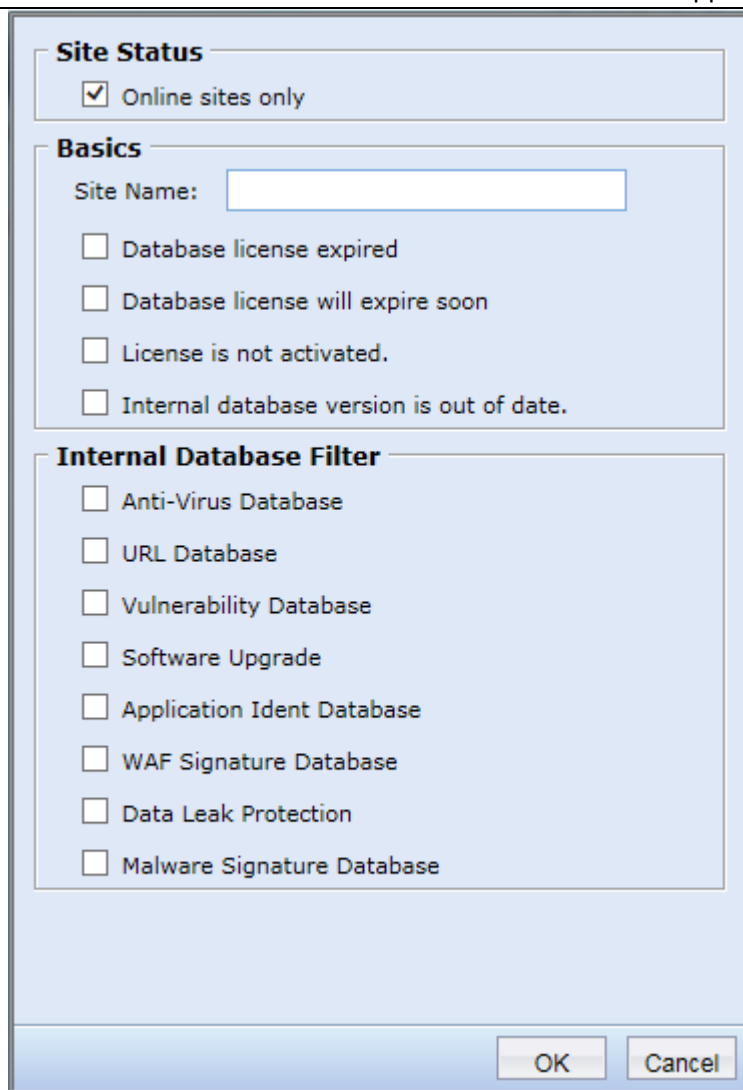
[Sort by] : Select applications display based on sorting of inbound/outbound/bidirectional traffic flow amount.

4.1.3.4 Internal Database Status

[Internal Database Status] includes [Filter] and [CMC Internal Database Status] function modules. This page display all NGAF sites internal database status, which includes name, status, database name, current version, latest version update service expiration and last reported. Date as shown below:

>>Internal Database Status							
Refresh Filter CMC Internal Database Status							
No.	Site Name	Status	Database Name	Current Version	Latest Version	Update Service Expiration	Last Reported
1	CTI	Internal database has expi...	Malware Signature Dat...	20141108	20141115	20150619/00:00:00	2014-12-15 09:07:19
2	CTI	Normal	Anti-Virus database	20141020	20141020	20150619/00:00:00	2014-12-15 09:07:19
3	CTI	Normal	URL database	20141020	20141020	20150619/00:00:00	2014-12-15 09:07:19
4	CTI	Normal	Vulnerability Database	20141017	20141017	20150619/00:00:00	2014-12-15 09:07:19
5	CTI	Normal	Vulnerability Database	--	20141116	Never expire	2014-12-15 09:07:19
6	CTI	Normal	Application Ident Data...	20141017	20141017	20150619/00:00:00	2014-12-15 09:07:19
7	CTI	Normal	WAF Signature Database	20141017	20141017	20150619/00:00:00	2014-12-15 09:07:19
8	CTI	Normal	Data Leak Protection	20141011	20141011	20150619/00:00:00	2014-12-15 09:07:19

[Filter] : Filter sites by using selective options such as update status and etc. Click on **Filter** and the page below is shown:



Site Status

☒ Online sites only

Basics

Site Name:

☐ Database license expired

☐ Database license will expire soon

☐ License is not activated.

☐ Internal database version is out of date.

Internal Database Filter

☐ Anti-Virus Database

☐ URL Database

☐ Vulnerability Database

☐ Software Upgrade

☐ Application Ident Database

☐ WAF Signature Database

☐ Data Leak Protection

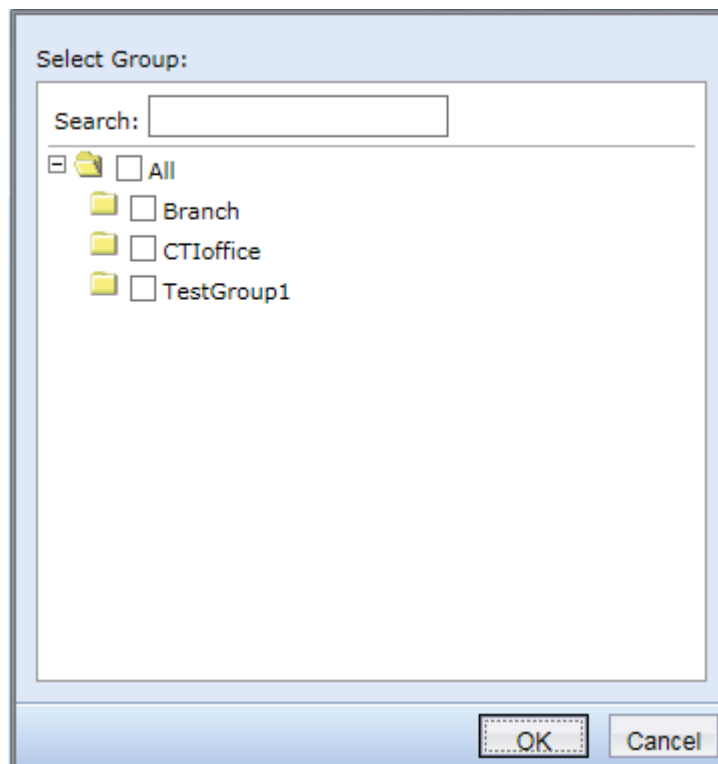
☐ Malware Signature Database

OK Cancel

[CMC Internal Database Status] : This module is used to check CMC internal database status which the databases is exactly same with NGAF. Click on the button, the following page is displayed:

[Stop] : Click on the button to stop all auto-update services, all NGAF sites will not be able to update via CMC.

[Filter] : The filter feature is used when there are many sites in order to narrow down the sites resulted by using selected parameters. Click on the button and the following figure is shown:



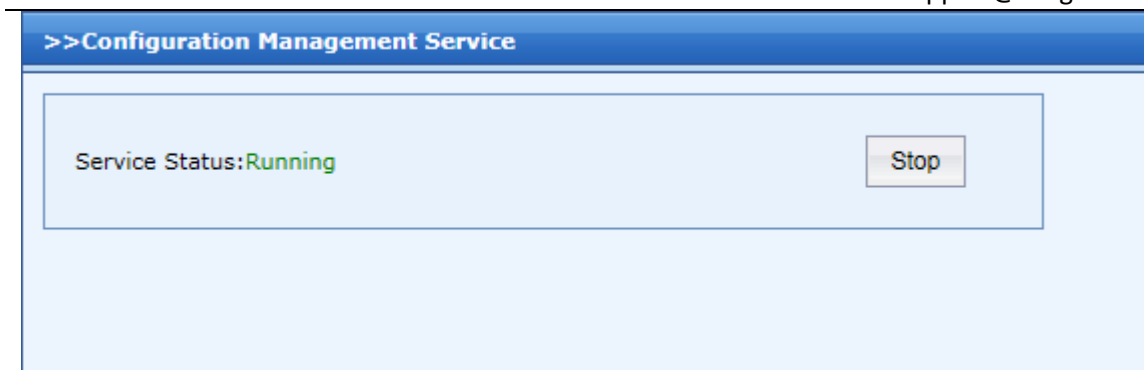
[Search] : Insert related group/sites name and click on **Search**, the search results will be displayed. Support fuzzy search but does not support wildcard search.

4.1.5. Services

[Services] includes [Configuration Management] and [TCP Proxy] function modules.

4.1.5.1 Configuration Management

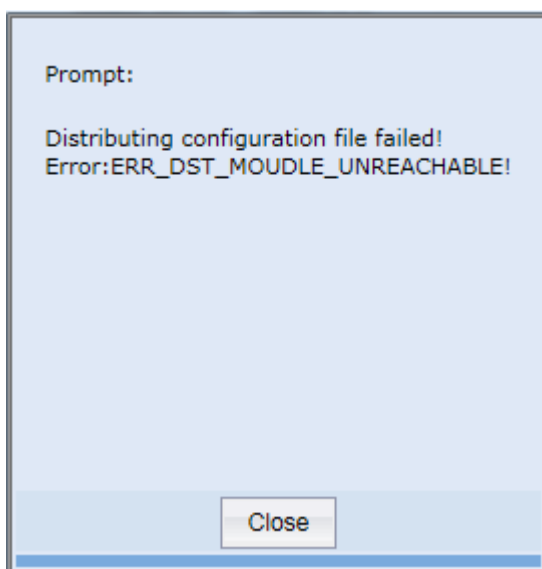
[Configuration Management] is used to manage CMC database



[Stop] : CMC will not able to distribute configuration to NGAF if the service is stop.

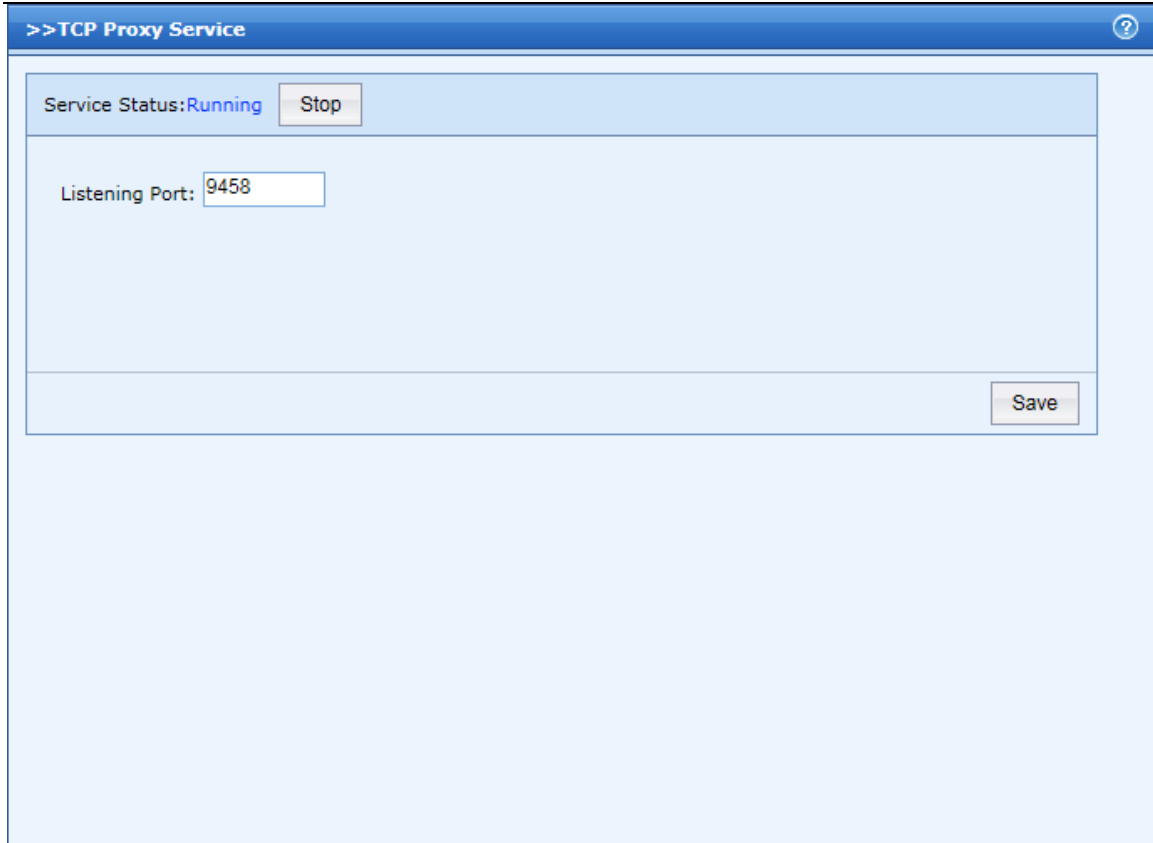


If the service is stop running, the error page below is prompted when distribute configuration to NGAF.



4.1.5.2 TCP Proxy

[TCP Proxy] is used for when NGAF connected to CMC, administrator select **Remote Control** via CMC's web console interface and browse to NGAF's related service with local 127.0.0.1 and proxy port. This enable administrator to remote control the NGAF even if the NGAF is not directly connected to CMC device (The process is similar to proxy service and thus is named as TCP Proxy). This feature does not need port forwarding or bypass in firewall but it requires only CMC device to open TCP port 9458(Factory default port) which is shown below:



[Stop] : Press on the button to terminate the service, CMC will not be able to visit NGAF via TCP Proxy.

[Listening Port] : CMC's listening port, configurable to any ports (But not ports which are already using in CMC to avoid conflict)



When CMC is deployed as single-arm mode, port forwarding need to be configured on the gateway device to port forward TCP 9458 (by default) to CMC device. If not, administrator will not be able to access to NGAF remote control sites via TCP Proxy in CMC's web console.

4.1.6. Logs

[Logs] includes [View] logs type, [Date] and [Filter] function modules. The feature is used to check on CMC's system logs and operation logs, the page is shown below:

>>Logs

Refresh Filter View: System logs Date: 20141216

Service	Severity	Time	Details
Communication Service	Info	10:22:22	[SaManager] Established file channel with CTI (L:0 R:0) successfully.
Communication Service	Info	10:22:20	[SaManager] File channel with CTI (L:0 R:0) is closed!
Communication Service	Info	10:12:19	[SaManager] Established file channel with CTI (L:0 R:0) successfully.
Communication Service	Info	10:12:15	[SaManager] File channel with CTI (L:0 R:0) is closed!
Communication Service	Info	10:02:14	[SaManager] Established file channel with CTI (L:0 R:0) successfully.
Communication Service	Info	10:02:12	[SaManager] File channel with CTI (L:0 R:0) is closed!
Communication Service	Info	09:52:11	[SaManager] Established file channel with CTI (L:0 R:0) successfully.
Communication Service	Info	09:52:07	[SaManager] File channel with CTI (L:0 R:0) is closed!
Communication Service	Info	09:42:07	[SaManager] Established file channel with CTI (L:0 R:0) successfully.
Communication Service	Info	09:42:03	[SaManager] File channel with CTI (L:0 R:0) is closed!
Config Manager	Info	09:42:00	[SCModule] Connect proxy success!
Config Manager	Info	09:42:00	(SCConfigManagerServer) Connect to proxy (ADDR:/var/sinfor/sc/scproxy_server))
Config Manager	Info	09:42:00	(SCConfigManagerServer) Config-dispatch service starts normally, version: 4.0.0.0, updated: Jul 20 2013 03:39:50
Config Manager	Info	09:40:42	(SCConfigManagerServer) Config-dispatch service stops normally
NTP Server	Info	09:30:26	(NTPSrv) System time deviates from NTP server time by -74 seconds.

Page 1 /15 Show page 1/15 Total 221 entries

[View] : Selectable options are system logs and operation logs. System logs show all CMC's services logs and Operation logs show the operations performed by CMC administrator.

>>Logs

Refresh Filter Advanced Search Search: View: Operation logs Date: 20141216

Administrator	Role	IP Address	Time	Module	Result	Operation Details
admin	Super admin	192.200.19.74	2014-12-16 10:35:59	User login	Succeeded	Log in
admin	Super admin	192.200.19.74	2014-12-16 10:25:33	User login	Succeeded	Log in
admin	Super admin	192.200.19.74	2014-12-16 09:42:02	System Mainte...	Succeeded	Start config-distribute service
admin	Super admin	192.200.19.74	2014-12-16 09:41:21	Terminal Mana...	Succeeded	Distribute config to site: CTI
admin	Super admin	192.200.19.74	2014-12-16 09:41:05	Terminal Mana...	Succeeded	Distribute config to group [1 sites]
admin	Super admin	192.200.19.74	2014-12-16 09:40:44	System Mainte...	Succeeded	Stop config-distribute service
admin	Super admin	192.200.19.74	2014-12-16 09:30:09	User login	Succeeded	Log in
Unknown user	Illegal	192.200.19.74	2014-12-16 09:30:04	User login	Failed	Log in

Page 1 /1 Show page 1/1 Total 8 entries

[Date] : Select date to view related logs on the particular day. By default, CMC can store up to 8 days for System logs and 90 days for Operation logs.



CMC's logs does not support synchronization or export to third party logging server.

[Refresh] : Click on the button to display the latest logs.

[Filter] : The feature is used to select logs based on filter options for both type of logs. The page are shown as below:



Filter Criteria -- Webpage Dialog

Log Severity

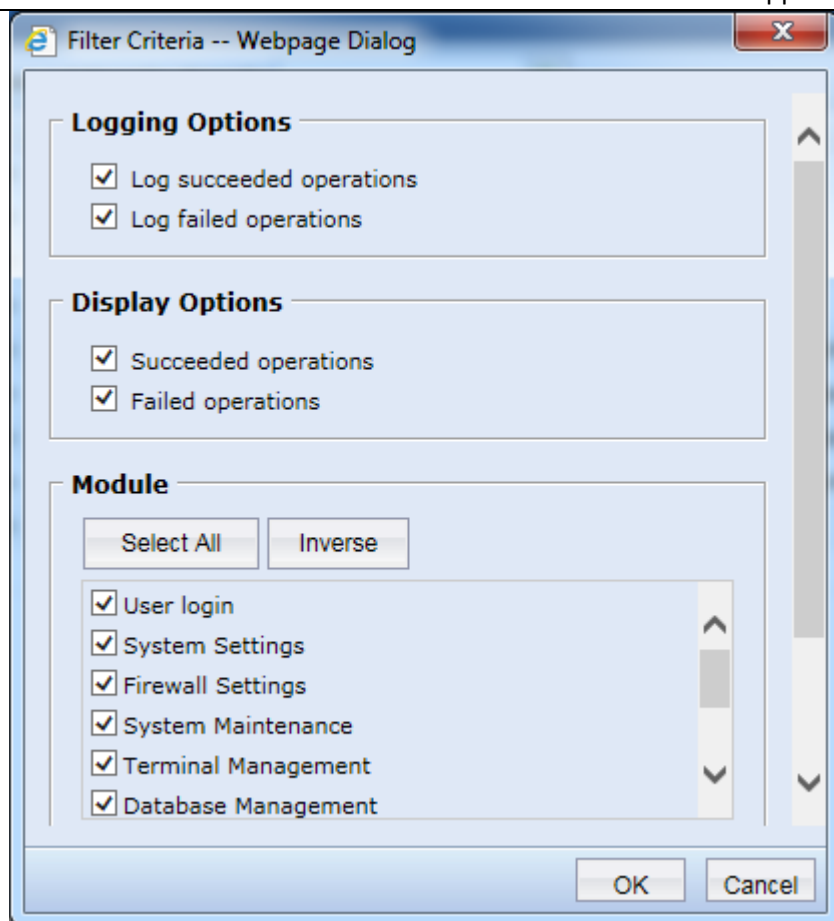
☒ Info ☒ Warning
☒ Error ☐ Debug

Entries Per Page: (10-1000)

Service Type

☒ Firewall
☒ Multiline Detection
☒ Anti-DoS
☒ Email Alarm
☒ Configuration Agent
☒ Info Exchange Background
☒ Communication Service
☒ VPN Extension
☒ TCP Proxy

For Operation logs, please refer to following page:

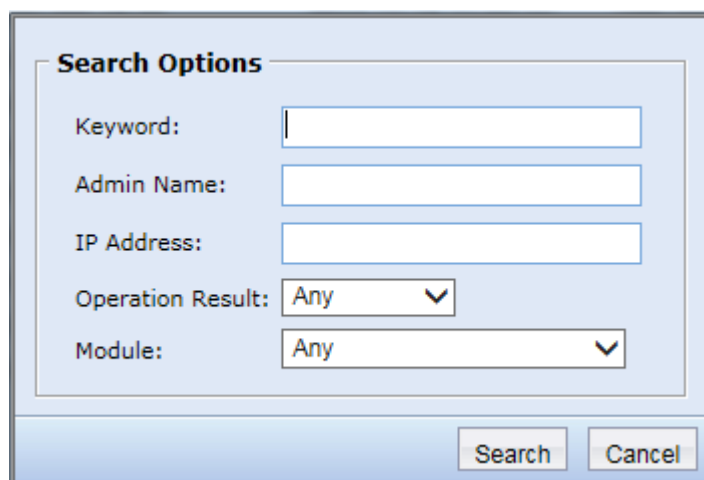


The dialog box titled "Filter Criteria -- Webpage Dialog" contains three sections: "Logging Options", "Display Options", and "Module".

- Logging Options:** Includes checkboxes for "Log succeeded operations" and "Log failed operations", both of which are checked.
- Display Options:** Includes checkboxes for "Succeeded operations" and "Failed operations", both of which are checked.
- Module:** Includes buttons for "Select All" and "Inverse", and a list of modules with checkboxes: "User login", "System Settings", "Firewall Settings", "System Maintenance", "Terminal Management", and "Database Management". All checkboxes are checked.

At the bottom right are "OK" and "Cancel" buttons.

[Advanced Search] : Search method which is only available for Operation logs. Key in information in the related fields to narrow down the logs display. The page is shown below:



The "Search Options" dialog box contains the following fields:

- Keyword:** A text input field.
- Admin Name:** A text input field.
- IP Address:** A text input field.
- Operation Result:** A dropdown menu with "Any" selected.
- Module:** A dropdown menu with "Any" selected.

At the bottom right are "Search" and "Cancel" buttons.

Users can choose to view different type of logs according to their need.

4.1.7. Config Distribution Status

[Config Distribution Status] is used to check the status when CMC distributing configuration, normally when editing NGAF sites configuration and click ok, the configuration will be distribute immediately to the remote control sites. If NGAF remote control sites are not connected to CMC or CMC's service is stopped, all synchronization logs will be displayed. The page is shown below:

>>Config Distribution Status						
Refresh						
Operation	Administrator	Site	Module	Result	Details	Time
distribute confi...	Admin	CTI	NGFW	Synchronizing succeeded	100%	2014-12-15 14:26:26
distribute confi...	Admin	CTI	CM	Synchronizing succeeded	100%	2014-12-15 14:26:26
distribute confi...	Admin	CTI	system	Synchronizing succeeded	100%	2014-12-15 14:26:26
distribute confi...	Admin	CTI	vpn	Synchronizing succeeded	100%	2014-12-15 14:26:26

[Refresh] : Click on the button to display the latest logs.



CMC's web console will prompt out a small windows which indicates synchronization/configuration distribution failure; meanwhile NGAF sites will pop up an icon to indicates the message during configuration upload.

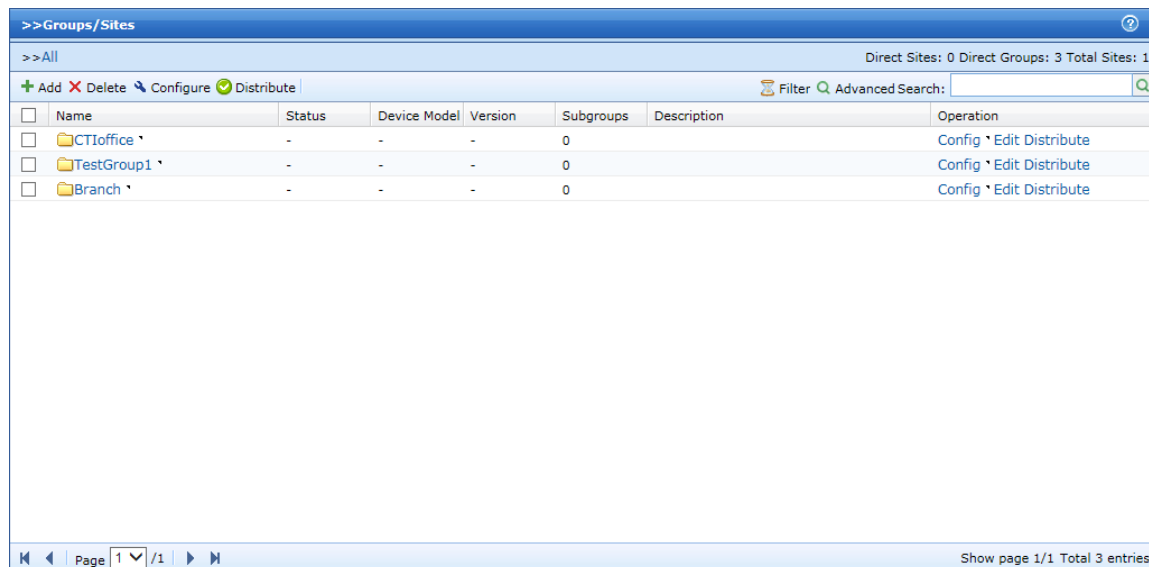
4.2. Site Management

This section include [Group/Sites], [TCP Proxy], [Scheduled Tasks], [Update Packages] and [Central Management] modules.

4.2.1. Groups/Sites

[Gourps/Sites] is used to differentiate groups and sites, can place NGAF devices into a group, group can include more groups. CMC administrator can manage NGAF devices via groups and sites

and this method can reduce the workload. The page is shown as below:



Name	Status	Device Model	Version	Subgroups	Description	Operation
CTIOffice	-	-	-	0		Config * Edit Distribute
TestGroup1	-	-	-	0		Config * Edit Distribute
Branch	-	-	-	0		Config * Edit Distribute

[Add] : Put the mouse cursor on the **Add** button, options [site], [Group], [Import site] and [Auto-generate site] is available. The page is shown below:



[Delete] : Click on **Delete** button to delete all selected groups/sites, unselected groups/sites will remain.

[Configure] : Click on the **Configure** button beside [Delete] can configure NGAF under ALL group which shown below:




[Distribute] : Click on the **Distribute** button beside [Configure] to distribute configuration to all current groups and NGAF sites.

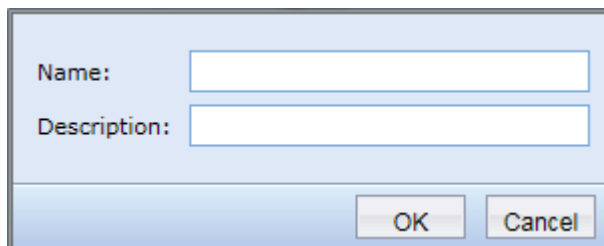
[Filter] : Can select single NGAF sites account for further actions.

[Advanced Search] : Can insert sites account to perform searching, supports fuzzy search.

4.2.1.1 Add Group

When there are alot of sites, the sites can be managed by placing under group or several groups.

Move the mouse cursor to the **Add** button, click on  **Group**, insert name and description to create a new group:



A dialog box for creating a new group. It has two text input fields: "Name:" and "Description:". At the bottom right, there are two buttons: "OK" and "Cancel".

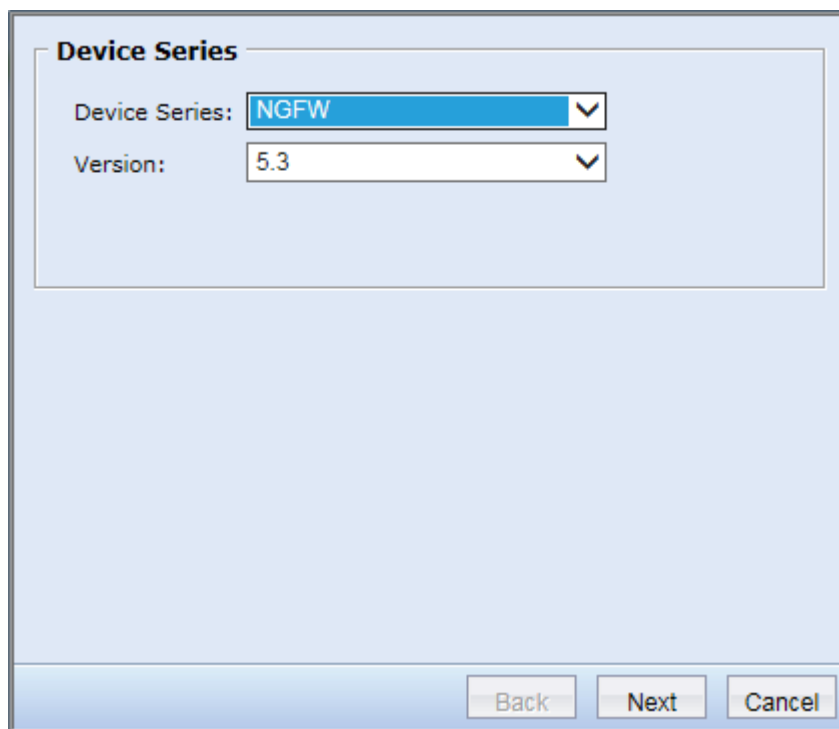


Group's details are not able to be modified after creation. If there is mistake found in group details, delete the group and re-create it.

By default, CMC device has only one ALL group, and it can not be deleted. Refer to Chapter 5 for more details

4.2.1.2 Add Sites

NGAF remote control sites can be created under ALL group or any other groups, it can be differentiate base on user's need. The page is shown below:



A dialog box titled "Device Series". It contains two dropdown menus: "Device Series:" with "NGFW" selected, and "Version:" with "5.3" selected. At the bottom, there are three buttons: "Back", "Next", and "Cancel".

Refer to Chapter 5 for more details

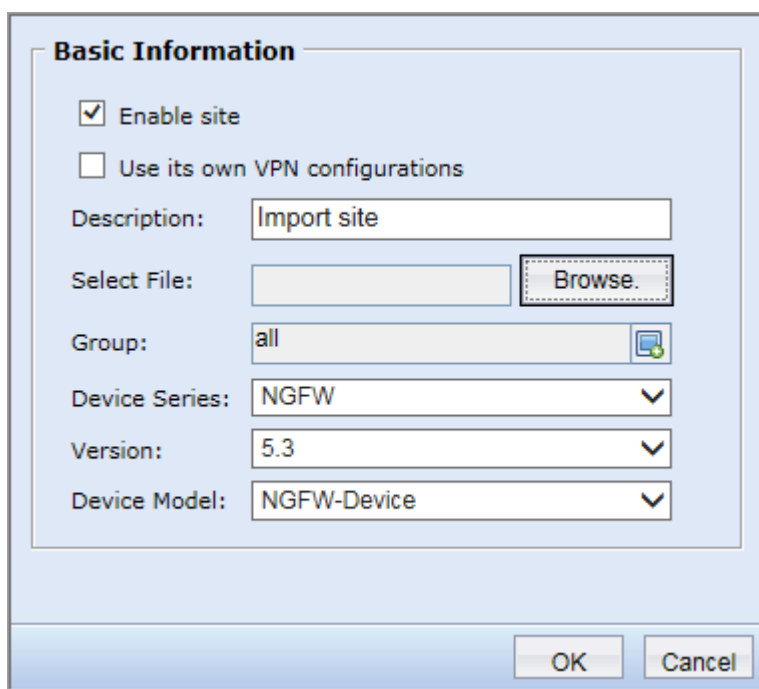
4.2.1.3 Import Site

Other than add groups/sites manually, we can use another method which is to import the sites from a file in order to reduce the workload if there are a lot of sites to be added. The case below shows steps to import sites:

Case : How to import sites

This case will describe how to import 3 sites into CMC under group ALL.

Move the mouse cursor to **Add** and select [Import Sites], the page below is shown:

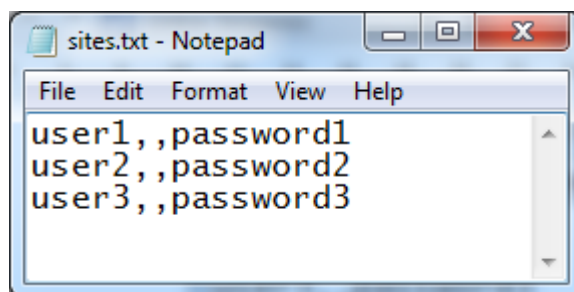


The dialog box titled "Basic Information" contains the following fields and options:

- ☒ Enable site
- ☐ Use its own VPN configurations
- Description:
- Select File:
- Group:
- Device Series:
- Version:
- Device Model:

At the bottom right are and .

[Browse] : Choose related file via this button, txt or .csv file. The content in the file should be as below:



sites.txt - Notepad

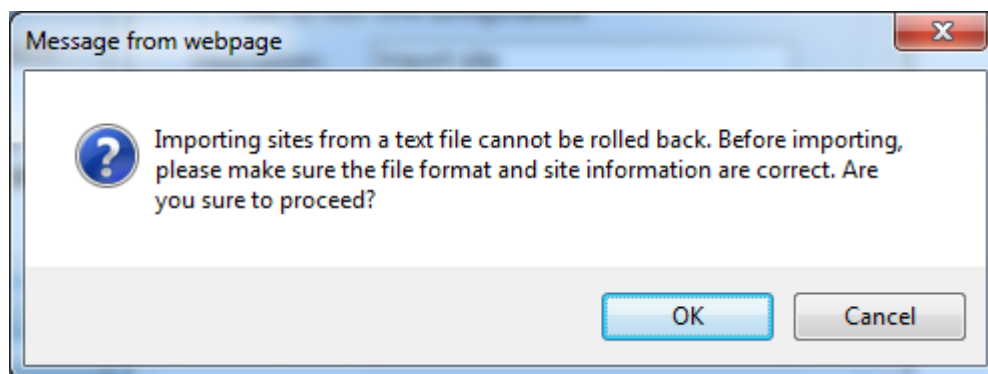
File Edit Format View Help


```
user1, ,password1
user2, ,password2
user3, ,password3
```

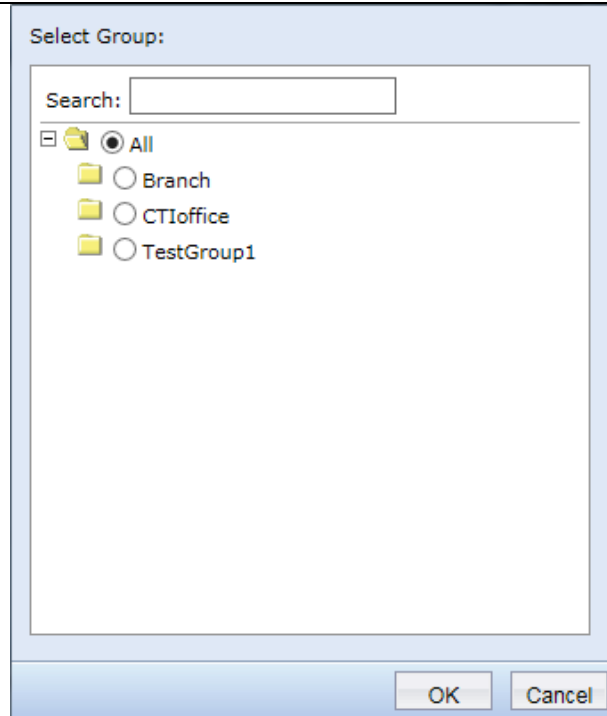


Warning :There are 2 commas between username and password.

Click on **Browse** and the page below is shown:



[Group] : Select the group which the sites import to. Click on  to select related group as shown below:



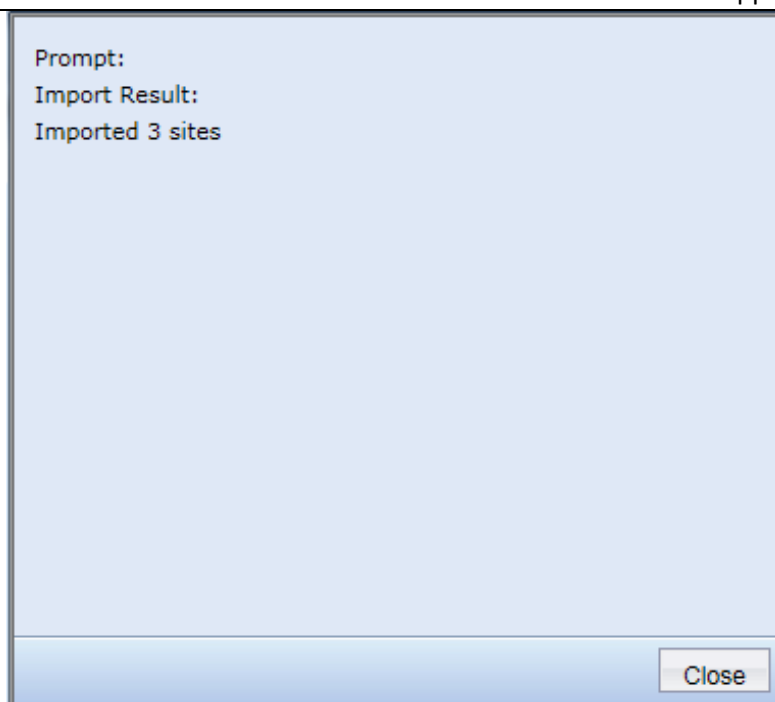
[Description] : Self-definable.

[Device Series] : remote control sites device

[Version] : The firmware version of remote control sites device.

[Device Model] : The hardware model of remote control sites device.

After done configuration, select **OK** to import the sites and the page below will be prompted if succeeded:



The sites will be shown in the related group (which is group ALL in this case) as below:

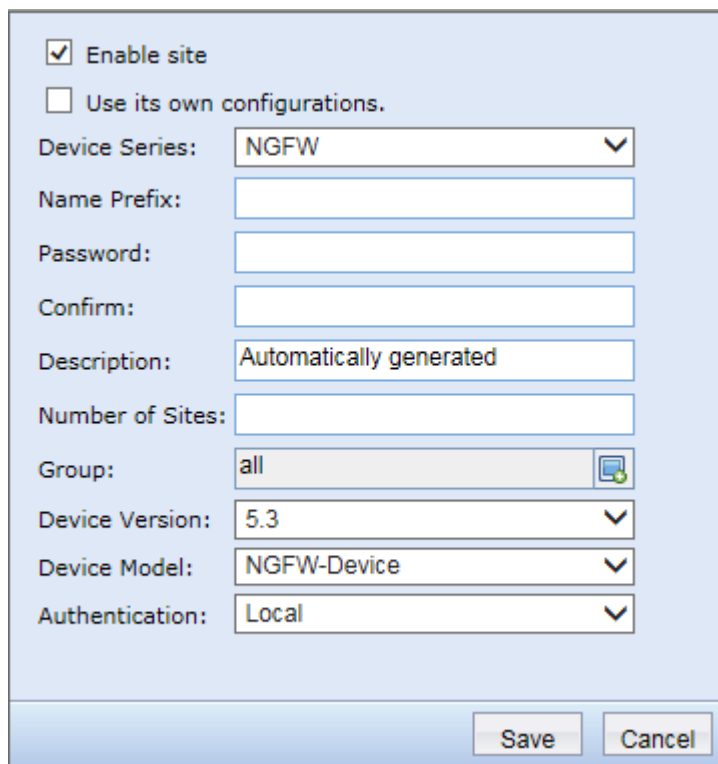
>>Groups/Sites							
>>All							
Direct Sites: 3 Direct Groups: 3 Total Sites: 4							
+ Add - Delete ⚙️ Configure ✅ Distribute ⌚ Filter 🔍 Advanced Search: <input type="text"/>							
<input type="checkbox"/>	Name	Status	Device Model	Version	Subgroups	Description	Operation
<input type="checkbox"/>	CTIoffice	-	-	-	0		Config * Edit Distribute
<input type="checkbox"/>	TestGroup1	-	-	-	0		Config * Edit Distribute
<input type="checkbox"/>	Branch	-	-	-	0		Config * Edit Distribute
<input type="checkbox"/>	user1	Enabled	NGFW-Device	NGFW 5.3	-	Import site	Config Edit Clone Distribute
<input type="checkbox"/>	user2	Enabled	NGFW-Device	NGFW 5.3	-	Import site	Config Edit Clone Distribute
<input type="checkbox"/>	user3	Enabled	NGFW-Device	NGFW 5.3	-	Import site	Config Edit Clone Distribute



Warning :The devices imported for each time must belongs to a same group, same device series and same version.

4.2.1.4 Auto-generate Site

Other than the two methods mentioned above, CMC can also auto-generate site by itself. The site which is auto-generated, its name are came with suffix. The page is shown below:



[Device Series] : remote control sites device

[Name Prefix] : Insert auto-generate sites name prefix

[Description] : Self-definable, default set to “Automatically generated”

[Number of sites] : The number of sites to be auto-generated.

[Group] : Select the group which the sites import to.

[Version] : The firmware version of remote control sites device.

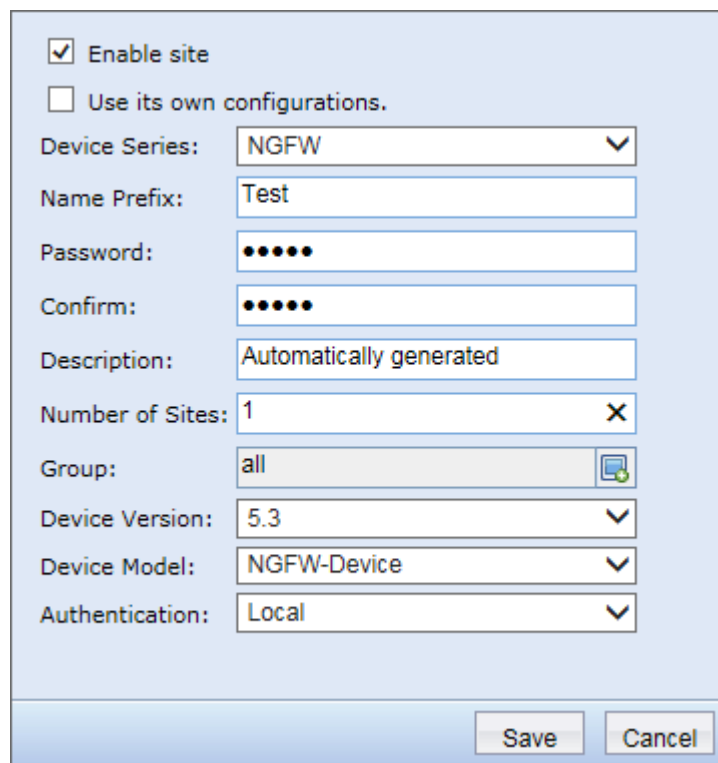
[Device Model] : The hardware model of remote control sites device.

[Authentication] : The authentication method using by auto-generate sites, select type Local normally unless there is LDAP or RADIUS server in local network, can synchronize with username and password in servers.

Case: How to configure auto-generate sites

This case describe how to create 1 auto-generate site under group ALL.

Move the mouse cursor to **Add** and select [Auto-generate sites], the page below is shown:



☒ Enable site
☐ Use its own configurations.

Device Series: NGFW

Name Prefix: Test

Password: •••••

Confirm: •••••

Description: Automatically generated

Number of Sites: 1

Group: all

Device Version: 5.3

Device Model: NGFW-Device

Authentication: Local


Save Cancel

This example need to create 1 auto-generated site under group ALL, refer to figure above for configuration, click on **Save** to create site Test1 as shown below:

Prompt:
 Created 1 sites

Close

>>Groups/Sites							
>>All							
Direct Sites: 4 Direct Groups: 3 Total Sites: 5							
+ Add X Delete ⚙ Configure ✓ Distribute Filter 🔍 Advanced Search: <input type="text"/>							
<input type="checkbox"/>	Name	Status	Device Model	Version	Subgroups	Description	Operation
<input type="checkbox"/>	CTIoffice `	-	-	-	0		Config * Edit Distribute
<input type="checkbox"/>	TestGroup1 `	-	-	-	0		Config * Edit Distribute
<input type="checkbox"/>	Branch `	-	-	-	0		Config * Edit Distribute
<input type="checkbox"/>	user1	Enabled	NGFW-Device	NGFW 5.3	-	Import site	Config Edit Clone Distribute
<input type="checkbox"/>	user2	Enabled	NGFW-Device	NGFW 5.3	-	Import site	Config Edit Clone Distribute
<input type="checkbox"/>	user3	Enabled	NGFW-Device	NGFW 5.3	-	Import site	Config Edit Clone Distribute
<input type="checkbox"/>	Test1	Enabled	NGFW-Device	NGFW 5.3	-	Automatically generated	Config Edit Clone Distribute

 **Warning :**The sites auto-generated for each time must belongs to a same group, same device series and same version.

4.2.1.5 Edit Sites

Sites can be edited base on password changes, site's name modification and group changes. Click on **Edit** on the site's right side to perform the changes.

Case : How to edit sites

This case describe how to change site's password.

Click on site's **Edit** button and the page below is shown:



Basic Information

☒ Enable site
☐ Use its own VPN configurations

Site Name:

Password:

Confirm:

Description:

Group:

Device Model:

Type:

Version:

Authentication:

Modify the password column in the dialog windows, then click on **Next** and **OK**.

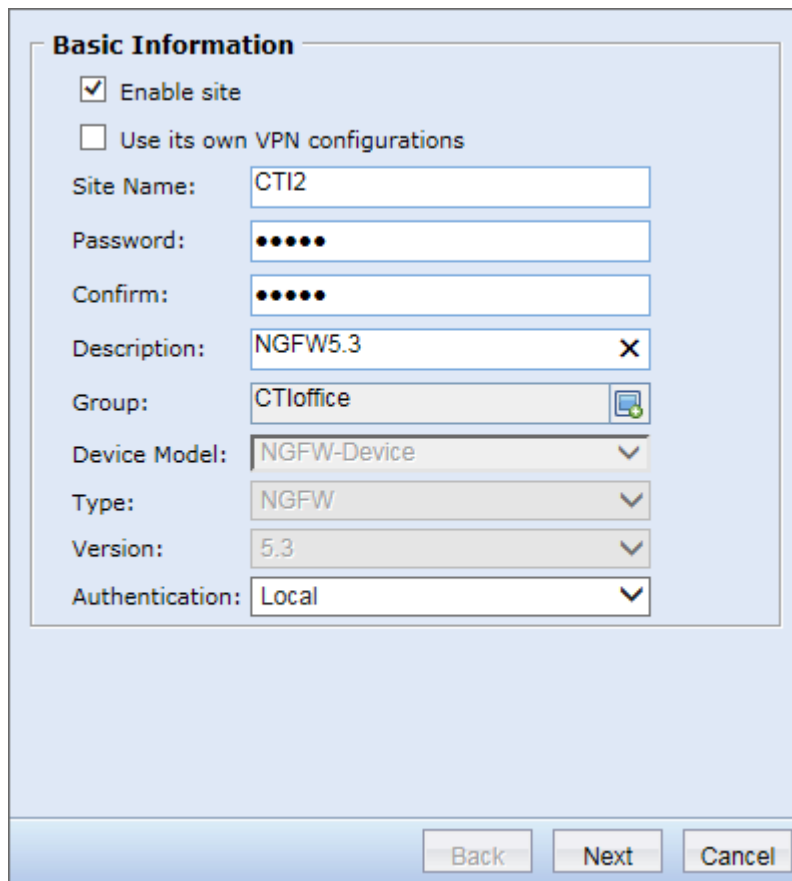
4.2.1.6 Clone Sites

When creating a new site, the site's group, device series and version same with another existing account, can use Clone to create the new site to ease user.

Case : How to clone sites

This case describe how to clone a NGAF site for another NGAF new site.

Click on **Clone** of the related site's right side and the following page is shown:



The dialog box titled "Basic Information" contains the following fields and controls:

- ☒ Enable site
- ☐ Use its own VPN configurations
- Site Name: CTI2
- Password: •••••
- Confirm: •••••
- Description: NGFW5.3
- Group: CTIoffice
- Device Model: NGFW-Device
- Type: NGFW
- Version: 5.3
- Authentication: Local

At the bottom, there are three buttons: Back, Next, and Cancel.

Insert all related information into the columns, then click on **Next** and **OK**.

4.2.1.7 Configure Sites

NGAF sites configurations divided into three types: Group NGAF configuration, Sites NGAF configuration and remote local NGAF configuration. When there are conflicts occur between config files, the sequence to prioritize is : Group NGAF Config > Sites NGWF Config > remote local NGAF Config.

By refer to the configuration properties, we will categorize the configuration into three types and different manage policy is apply on each type:

[Mergeable Config] : Group, Sites and remote local NGAF config are available in the CMC device. For example, NGAF's security policy module is merge type config, when Group configured with security policy A, remote local config is configured with security policy B, both policy A and policy B can be seen on the NGAF.

[Switchable Config] : The groups/sites' config has higher priority compare to remote local config. For example: NGAF's anti-virus policy is a switchable configuration, when group NGAF enable anti-virus policy but remote local NGAF disable it, by default, the anti-virus policy is enabled.

[Local Config] : Only a few configuration can be allowed in remote local config, for example, network zone configuration, real-time status and etc. The module which included in this config is [Real-time Status], [Bandwidth Management], [Virtual Line], [SNAT], [DNAT] and [Network].

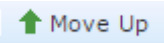


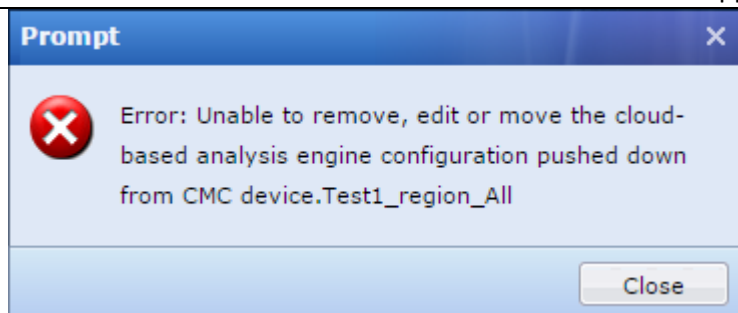
Some Mergeable type config have priority order, these distributed config will work in order: Group > Site > local, the local config policy cannot take over the priority of group config policy.

Application Control Policy

CM Info Bar The configuration pushed down from CMC device cannot be edited. You can edit local configuration only.

<

If click on the  when selecting local policy to re-order the policy, the system will prompt error message as shown below:



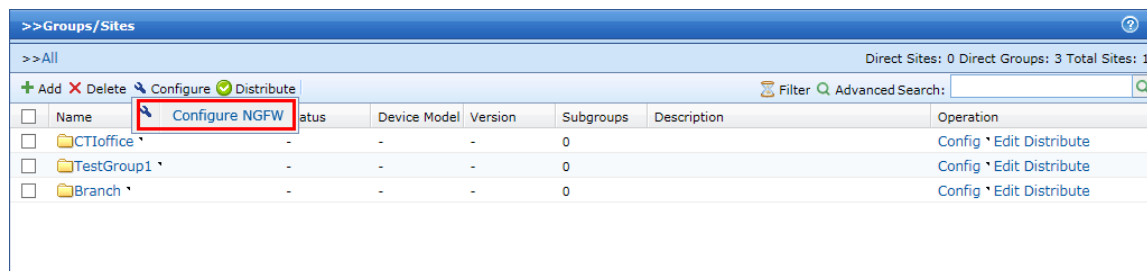
The following details describe the type of configuration and a variety of application scenarios for each configuration :

NGAF Group ALL Config access method

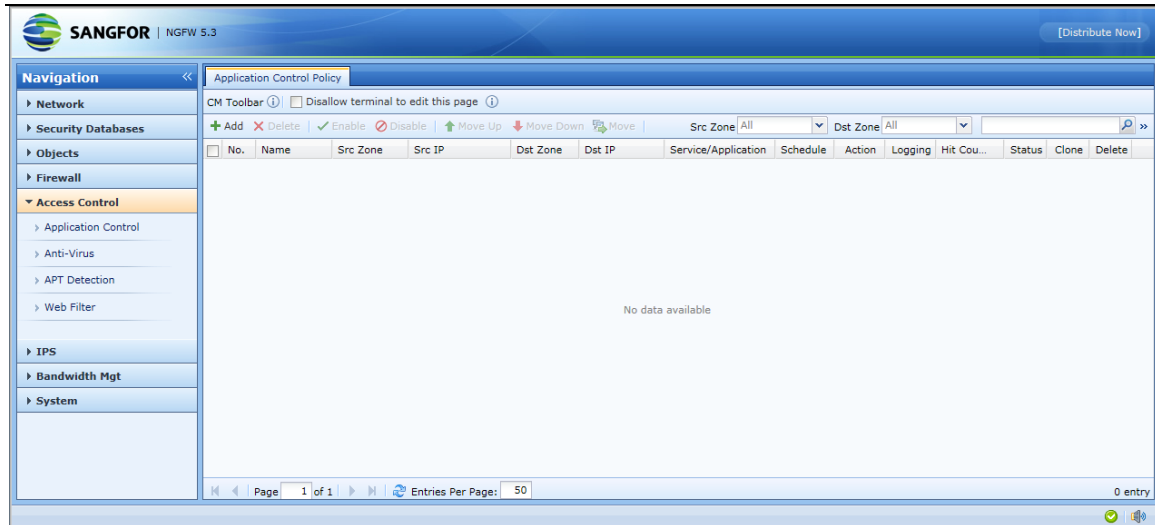
This config type has the highest priority among all other config types and will distribute to all groups and all sites.

Case : Configure NGAF in Group ALL

Move the mouse cursor to **Configure** and select [Configure NGAF] as shown in the following page:



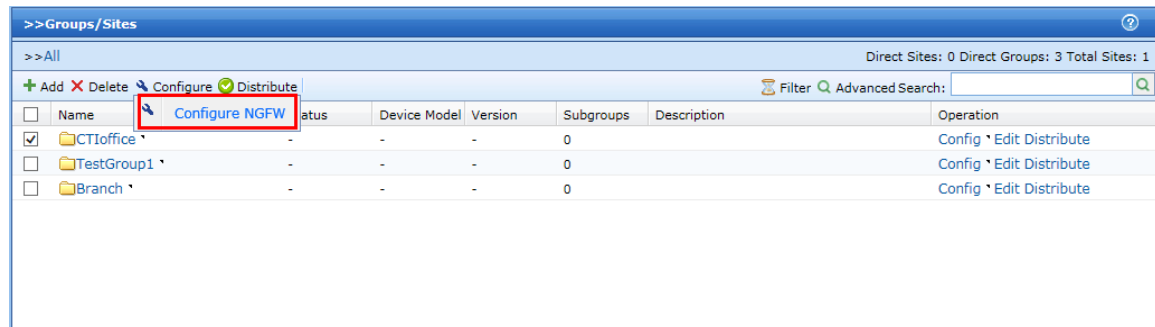
The page will be redirect to another page as shown below:



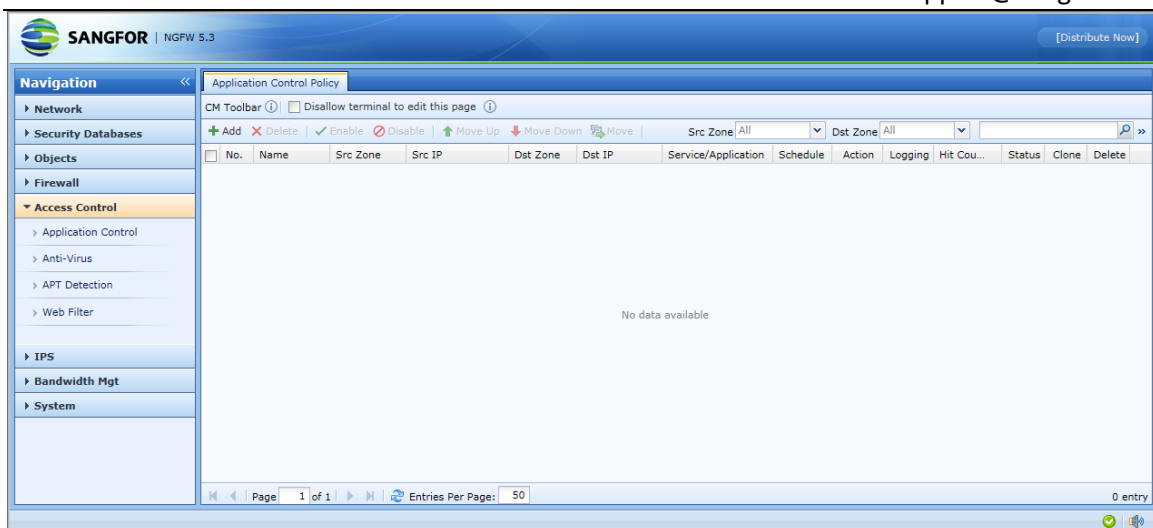
NGAF Group Config access method

Case : Configure NGAF in Group

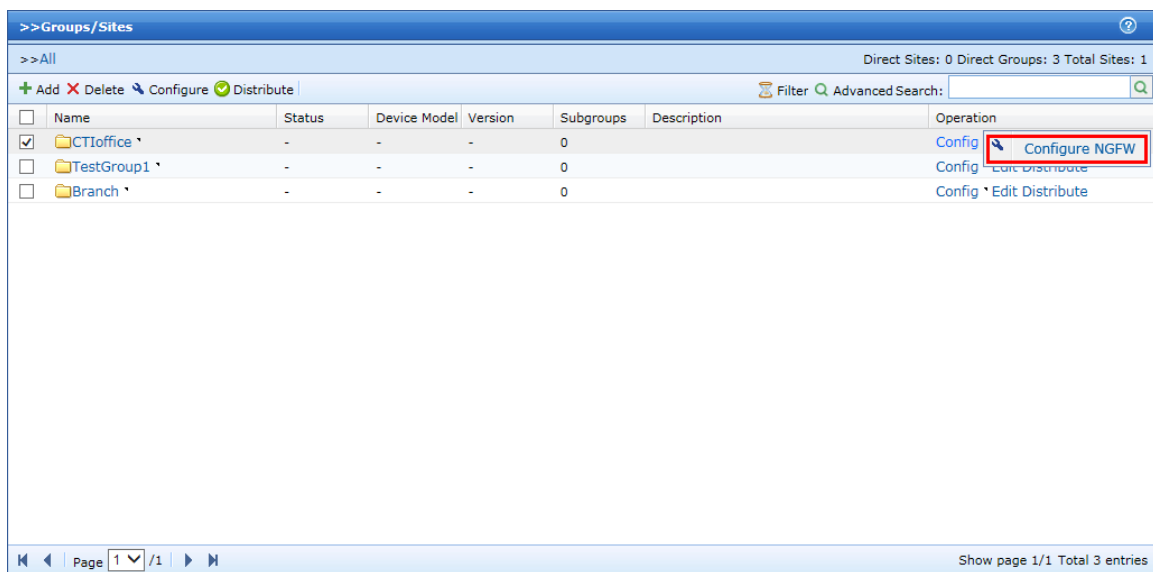
Method 1 : Move the mouse cursor to **Configure** and select [Configure NGAF] as shown in the following page:



The page will be redirect to another page as shown below:



Method 2 : Move the mouse cursor to **Configure** and select [Configure NGAF] on the right side of Group as shown in the following page:



NGAF Sites Config access method

Case : Configure NGAF under NGAF sites

Method 1 : Move the mouse cursor to the related site and click on it as shown below:

>>Groups/Sites

>>All>>CTIOffice Direct Sites: 1 Direct Groups: 0 Total Sites: 1

+ Add X Delete Configure Distribute Filter Advanced Search: []

<input type="checkbox"/>	Name	Status	Device Model	Version	Subgroups	Description	Operation
<input checked="" type="checkbox"/>	CTI	Enabled	NGFW-Device	NGFW 5.3	-		Config Edit Clone Distribute

Page 1 / 1 Show page 1/1 Total 1 entries

The page will be redirected to page below:

SANGFOR NGFW 5.3 [Distribute Now]

Navigation <<

- Network
- Security Databases
- VPN
- Objects
- Firewall
- Access Control
 - Application Control
 - Anti-Virus
 - APT Detection
 - Web Filter
- IPS
- Bandwidth Mgt
- System

Application Control Policy

CM Toolbar [] Disallow terminal to edit this page [] CM Advanced Options

+ Add X Delete Enable Disable Move Up Move Down Move

Src Zone All Dst Zone All

No.	Name	Src Zone	Src IP	Dst Zone	Dst IP	Service/Application	Schedule	Action	Logging	Hit Cou...	Status	Clone	Delete
No data available													

Page 1 of 1 Entries Per Page: 50 0 entry

Method 2 : Click on the **Config** on the right side of the site's name as shown below:

>>Groups/Sites							
>>All>>CTIOffice				Direct Sites: 1 Direct Groups: 0 Total Sites: 1			
+ Add X Delete Configure Distribute				Filter Advanced Search			
<input type="checkbox"/>	Name	Status	Device Model	Version	Subgroups	Description	Operation
<input checked="" type="checkbox"/>	CTI	Enabled	NGFW-Device	NGFW 5.3	-		Config Edit Clone Distribute

NGAF Sites Configuration Introduction:

Network Configuration

[Interface]

Module Description : The configuration in this page is local config, it has to be done by remote NGAF itself.

[Advanced]

Module Description : The configuration under this page is switchable config. User can configure SNMP and SNMP related switch option, only available in sites configuration, group configuration does not include this page.

CMC toolbar instructions:

NGAF Sites page in CMC is shown as below:

Advanced Options												
CM Toolbar ⓘ <input type="checkbox"/> Disallow terminal to edit this page ⓘ <input type="checkbox"/> Push SNMP change down to terminal ⓘ <input type="checkbox"/> CM Advanced Options												
SNMP <input checked="" type="checkbox"/> Enable SNMP												
SNMP << > SNMP V1/V2 > SNMP V3 > SNMP Trap	SNMP V1/V2 + Add X Delete Refresh <table border="1"> <thead> <tr> <th>Name</th> <th>IP Address</th> <th>Community</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td colspan="4"> </td> </tr> </tbody> </table>				Name	IP Address	Community	Delete				
Name	IP Address	Community	Delete									

Check the [Push SNMP change down to terminal] to distribute the configuration of this page to

remote NGAF devices. Check the [High Priority] in CM Advanced Options, the configuration on this CMC page will have higher priority than the local configuration.

Security Databases

Module description : The configuration on this page is under local NGAF config category. The configuration is done in local devices. The page on CMC is used to check the content of these security databases which includes [Vulnerability], [WAF Signature], [Data Leak Protection] and [Malware Signature]. The menu is shown in figure below:

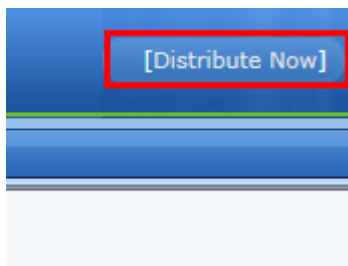


VPN

Module description : This module is used to configuration VPN for NGAF devices. The module includes functions such as [Basics], [Local Users], [VPN Connections], [Virtual IP Pool], [VPN WAN Interface], [VPN LAN Interface], [Multiline Policy], [Local Subnet], [Tunnel Route], [IPSec VPN], [Objects] and [Advanced].The page is shown as following:



Refer to NGAF User Manual 5.3 under VPN section for configuration details. After done configured this section, select [Distribute Now] on the top right of the page to distribute the configuration to related NGAF device as shown in the figure below:



Objects

Module description : This module describe the objects used in access control policy or any related policy in NGAF device config. For details, refer to NGAF5.3 User Manual under section Objects.

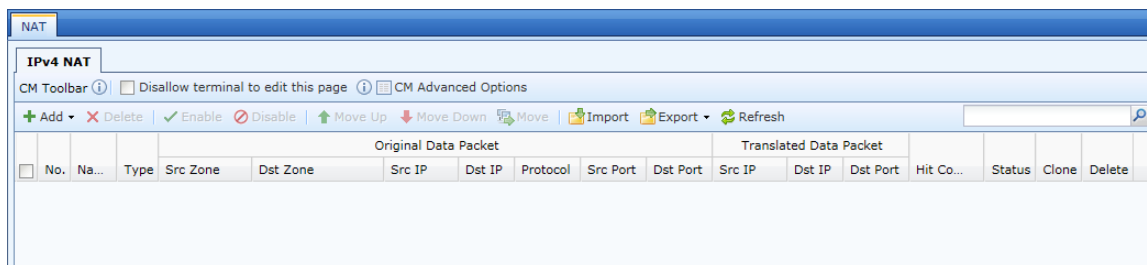
Firewall

[NAT]

Module description : This module only visible in site's user interface and belongs to Mergeable type NGAF config. The final configuration is consisted of both CMC and NGAF local config.

CMC toolbar instructions:

NGAF Sites page in CMC is shown as below:



Check the option [Disallow terminal to edit this page] to disable the local terminal to change configuration for this page in the NGAF device. Select the [Do not push configuration down to terminal] under [CM Advanced options] to prevent the current configuration on this page to be distributed to the local NGAF device.

Access Control

Module description : Network security issues come in when local users has unlimited access control to any website or any source, therefore NGAF can protect local resource via [Application Control], [Anti-Virus], [APT Detection] and [Web Filter] modules. The page is shown as below:



[Application Control] : Mergeable type NGAF config, filter traffics base on application layer and also port used.

[Anti-Virus] : Switchable type NGAF config, is used to detect virus and block if necessary; protect traffics and data from/to configured zone in NGAF.

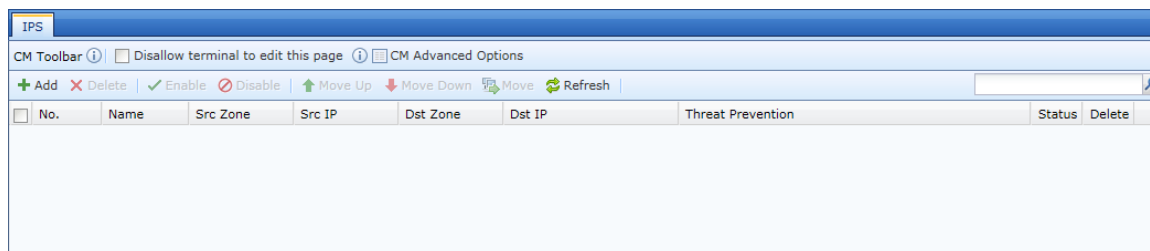
[APT Detection] : Mergeable type NGAF config, is used to detect local malware, trojan and harmful application/software. Block and logging (base on user's configuration) if infected software trying to communicate with public network.

[Web Filter] : Mergeable type NGAF config, this module is used to filter website browsing data which mainly are [URL Filter] and [File Filter].

IPS

Module description : Mergeable type NGAF config, can be configured only in site's config and

remote local config. Intrusion Prevention System rely in the packets detection to discover potential threats to the internal network systems. IPS will check internal network packets to ensure the real purpose of the packets, then it will decide whether to allow or deny these packets to internal network base on user's configuration.



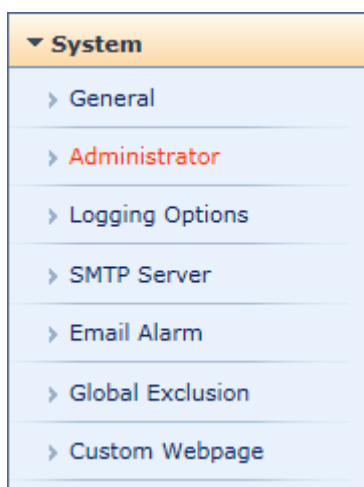
Refer to NGAF User Manual 5.3 under IPS section for configuration details.

Bandwidth Management

Module description : The main usage for this module is to control the bandwidth usage in NGAF. For details, refer to NGAF User Manual 5.3 under Bandwidth Management section.

System

Module description : Include all basic system configuration, the page is shown as following:



[General] : Switchable NGAF config, used to configure network settings.

[Administrator] : Switchable NGAF config, used to configure administrator account, CMC can only change administrator account's password.

[Logging Options] : Switchable NGAF config, used to configure settings for internal data center, syslog and logging options in NGAF.

[SMTP Server] : Switchable NGAF config, used to configure mail server which send warning or alarm email.

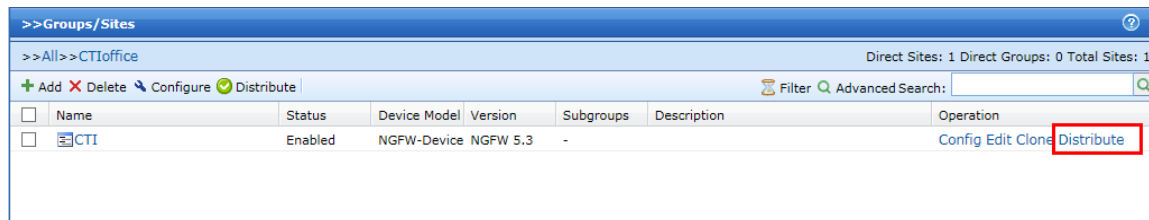
[Email Alarm] : Switchable NGAF config, used to inform admin via alarm email.

[Global Exclusion] : Mergeable NGAF config, used to exclude target host from being monitor, traffic filtering or any policies/bypass the host's traffic.

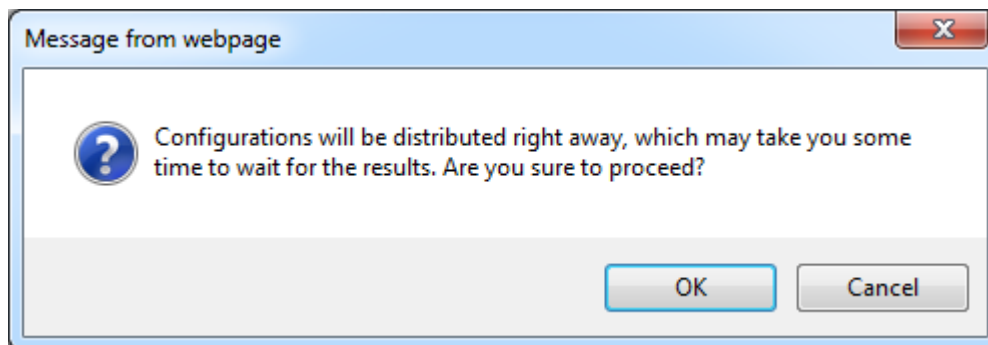
[Custom Webpage] : Switchable NGAF config, used to customize the webpage which redirect to host which include authentication result page, access denied page, virus found page, change password page, notice board page, web authentication page and user locked page.

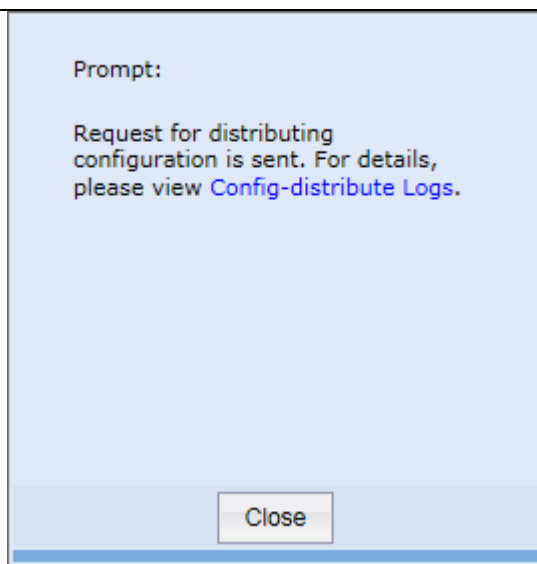
4.2.1.8 Distribute

After done configuration for NGAF sites/groups, by default CMC will distribute the configuration to all sites and groups for every 10 minutes. However, admin can click on **Distribute** if wanted to push the configuration to NGAF immediately. The page is shown below:



After click on the button, the following windows will prompt out:





After that, the result can be checked on the [Config-distribute Logs] as shown in the figure below:

>>Config Distribution Status						
Refresh						
Operation	Administrator	Site	Module	Result	Details	Time
distribute configura...	Admin	CT1	vpn	Synchronizing succeeded	100%	2014-12-17 16:39:15
distribute configura...	Admin	CT1	CM	Synchronizing succeeded	100%	2014-12-17 16:39:14
distribute configura...	Admin	CT1	system	Synchronizing succeeded	100%	2014-12-17 16:39:14
distribute configura...	Admin	CT1	NGFW	Synchronizing succeeded	100%	2014-12-17 16:39:14
distribute configura...	Admin	CT1	NGFW	Synchronizing succeeded	100%	2014-12-17 16:39:00
distribute configura...	Admin	CT1	system	Synchronizing succeeded	100%	2014-12-17 16:39:00
distribute configura...	Admin	CT1	CM	Synchronizing succeeded	100%	2014-12-17 16:39:00
distribute configura...	Admin	CT1	vpn	Synchronizing succeeded	100%	2014-12-17 16:39:00
distribute configura...	Admin	CT1	CM	Synchronizing succeeded	100%	2014-12-17 10:44:30
distribute configura...	Admin	CT1	NGFW	Synchronizing succeeded	100%	2014-12-17 10:44:30
distribute configura...	Admin	CT1	system	Synchronizing succeeded	100%	2014-12-17 10:44:30
distribute configura...	Admin	CT1	vpn	Synchronizing succeeded	100%	2014-12-17 10:44:30
distribute configura...	Admin	CT1	vpn	Synchronizing succeeded	100%	2014-12-17 09:48:14
distribute configura...	Admin	CT1	NGFW	Synchronizing succeeded	100%	2014-12-17 09:48:13
distribute configura...	Admin	CT1	system	Synchronizing succeeded	100%	2014-12-17 09:48:13
distribute configura...	Admin	CT1	CM	Synchronizing succeeded	100%	2014-12-17 09:48:13
distribute configura...	Admin	CT1	NGFW	Synchronizing succeeded	100%	2014-12-17 09:46:28
distribute configura...	Admin	CT1	vpn	Synchronizing succeeded	100%	2014-12-17 09:46:28
distribute configura...	Admin	CT1	system	Synchronizing succeeded	100%	2014-12-17 09:46:28
distribute configura...	Admin	CT1	CM	Synchronizing succeeded	100%	2014-12-17 09:46:28

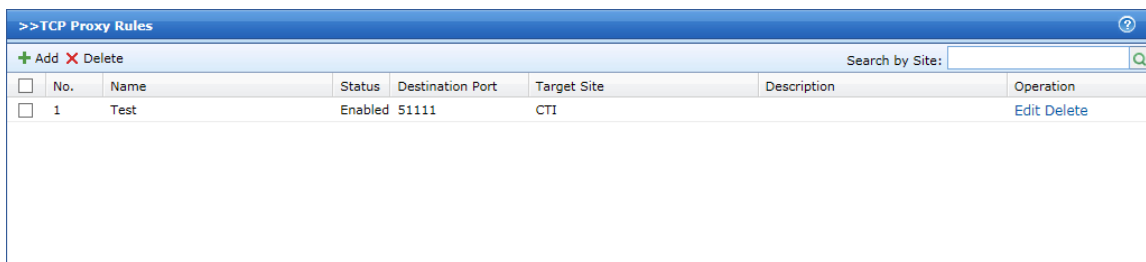


Ensure the databases of CMC and NGAF are having the same version, distribute operation might fail if the requirement does not met.

4.2.2. TCP Proxy

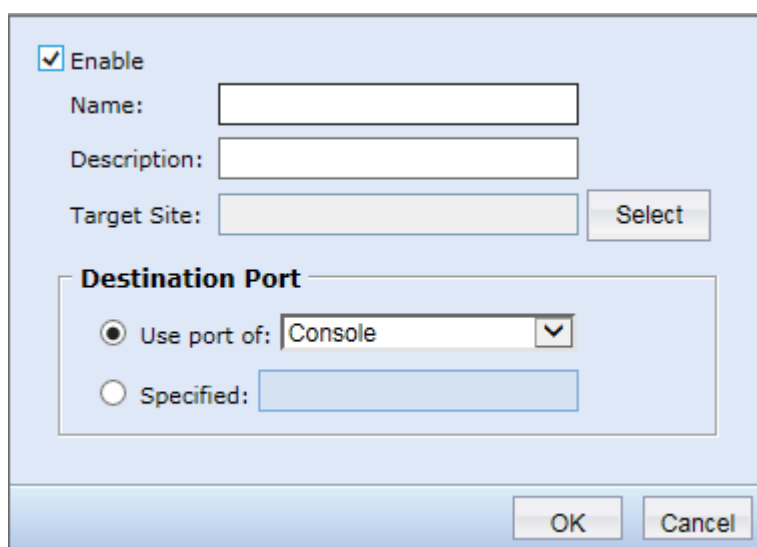
[TCP Proxy] module is used to enable connection between CMC and NGAF even though both devices are not connected directly (The process is similar to proxy service and thus is named as TCP Proxy). This feature does not need port forwarding or bypass in firewall but it requires only CMC

device to open TCP port 9458(Factory default port) and the port is changeable which is shown in the figure below:



No.	Name	Status	Destination Port	Target Site	Description	Operation
1	Test	Enabled	51111	CTI		Edit Delete

[Add] : Click on **Add** to create a new TCP proxy, the page is shown below:



☒ Enable

Name:

Description:

Target Site:

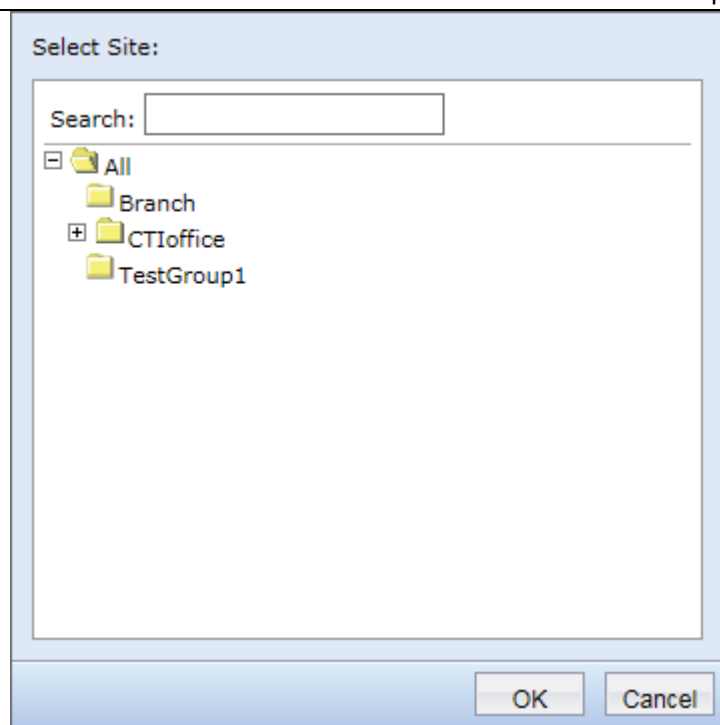
Destination Port

☒ Use port of:

☐ Specified:

[Name] and [Description] can be Self-define.

[Target Site] : Select related sites to apply TCP Proxy on, as shown below:



[Destination Port] : Select related services/ports for the NGAF sites which include known service ports and Self-define ports.

[Use port of] : Include Console and remote helping.

[Specified] : Self-define ports for selected NGAF sites.

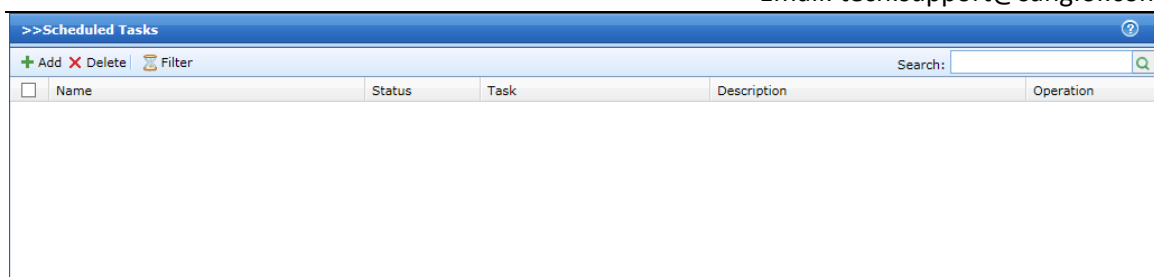
[Delete] : Click on **Delete** to remove the created TCP Proxy entry.



The real-time logs and remote maintenance in TCP Proxy service are reserved for commissioning services and the usage is not significant for user.

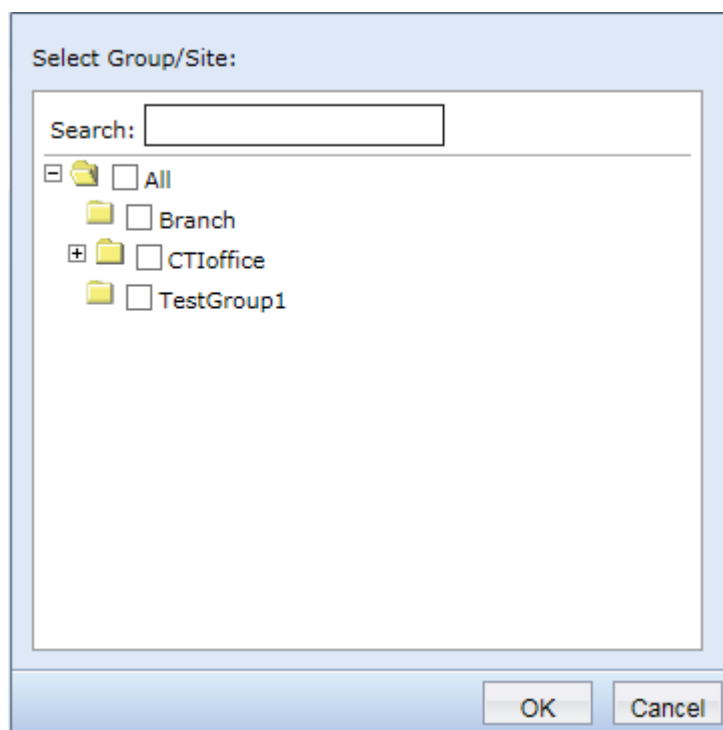
4.2.3. Schedule Tasks

[Schedule Tasks] module is used to add auto-update task for NGAF sites, the page is shown below:



[Delete] : Click to remove the created task.

[Filter] : Use the filter feature when there are many sites in order to narrow down the sites resulted by using selected parameters. Click on the button and the following figure is shown:

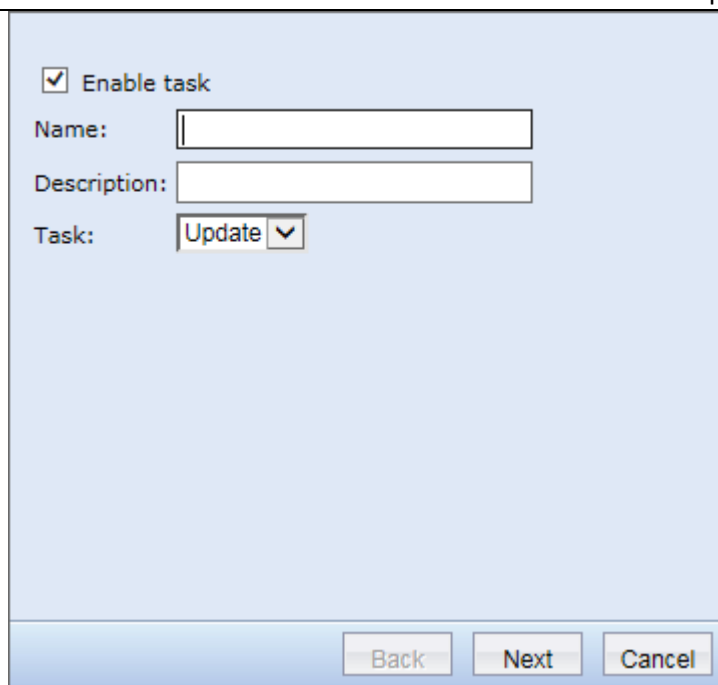


Select the related group and click **OK**.

[Search] : Insert related group/sites name and click on **Search**, the search results will be displayed.

Support fuzzy search but does not support wildcard search.

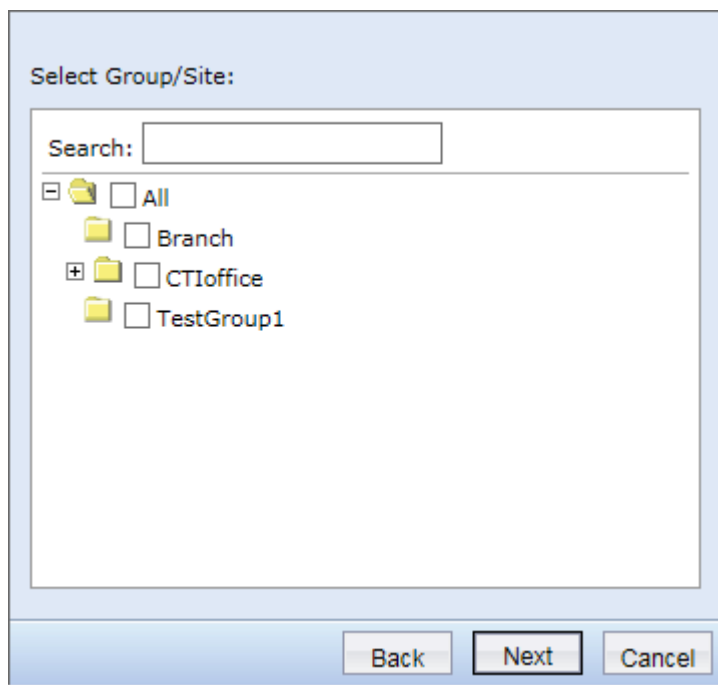
[Add] : Create a new task for site's auto-update, page is shown below:



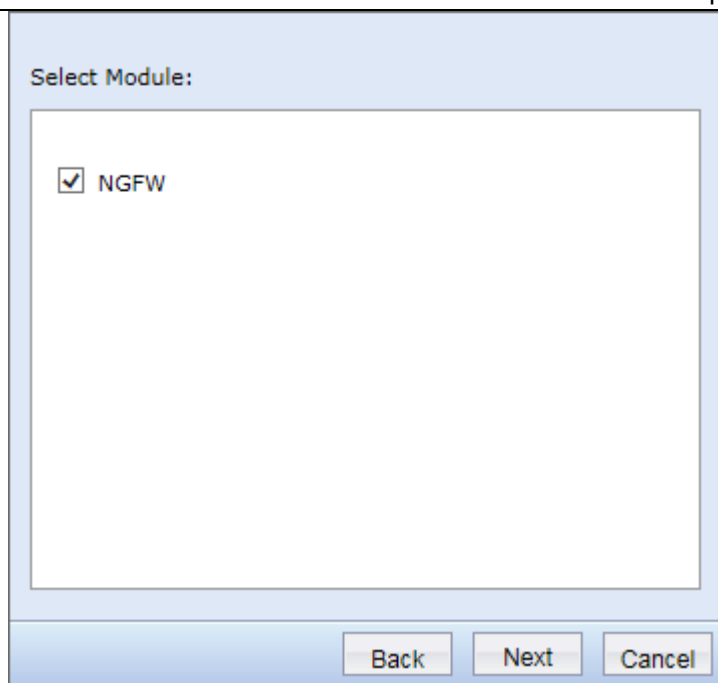
[Name] and [Description] can be Self-define.

[Task] : Update

Click on **Next** and the next page is shown as following:



Select the target sites and click on **Next**:

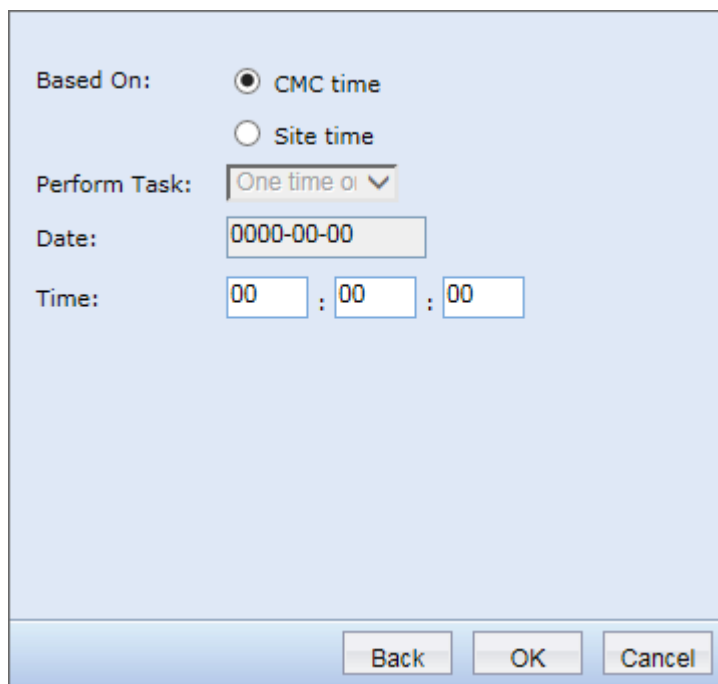


Select Module:

☒ NGFW

Back Next Cancel

Select [NGAF] and proceed to next page:



Based On: ☒ CMC time
☐ Site time

Perform Task: One time or ▼

Date: 0000-00-00

Time: 00 : 00 : 00

Back OK Cancel

Choose the proper date and time to perform the update, able to select base on [site time] or [CMC time] and click on **OK** to complete the configuration.



Warning : Task configuration will be checked by NGAF sites for every minute,



4.2.4. Update Packages





[illegible]

[Add] : Add a new update package, page is shown in the figure below:

Update Package:

Select Group/Site:

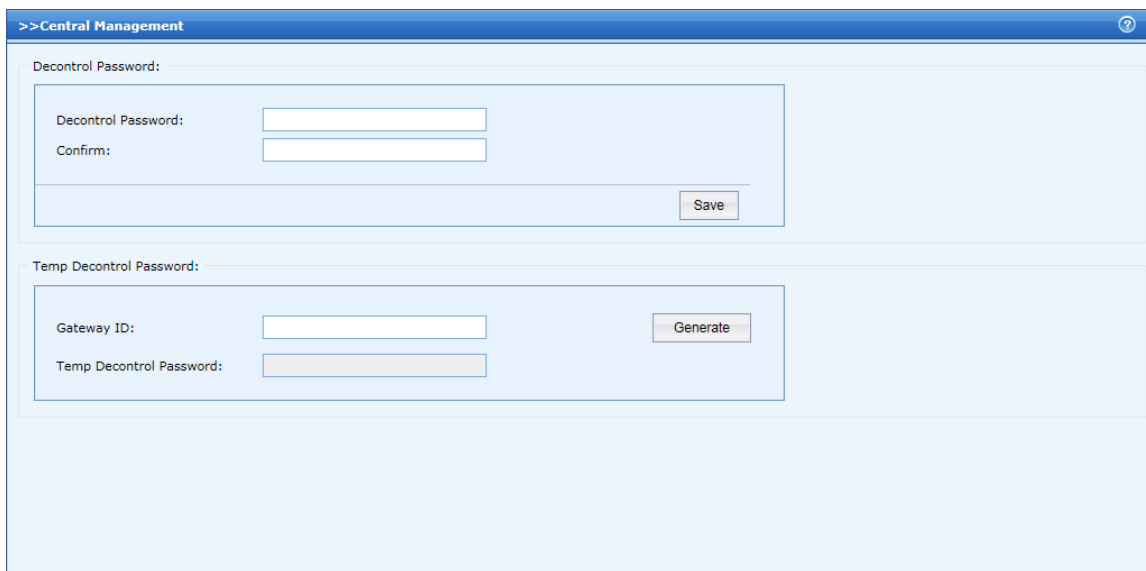
Search:

- ☐  ☐ All
- ☐  ☐ Branch
- ☒  ☐ CTIOffice
- ☐  ☐ TestGroup1

67

4.2.5. Central Management

After NGAF device joined to CMC sites, admin must use password to quit from CMC control. Use CMC's generated Temp Decontrol Password to remove the NGAF from CMC sites. The page is shown below:



[Decontrol Password] : Configure a password here and the password is working for all connected NGAF sites without expiry time unless admin change it.

[Temp Decontrol Password] : Require to insert NGAF gateway ID then CMC will generate a temporary password for the particular NGAF, valid until 24.00 of creation day.

4.3. System

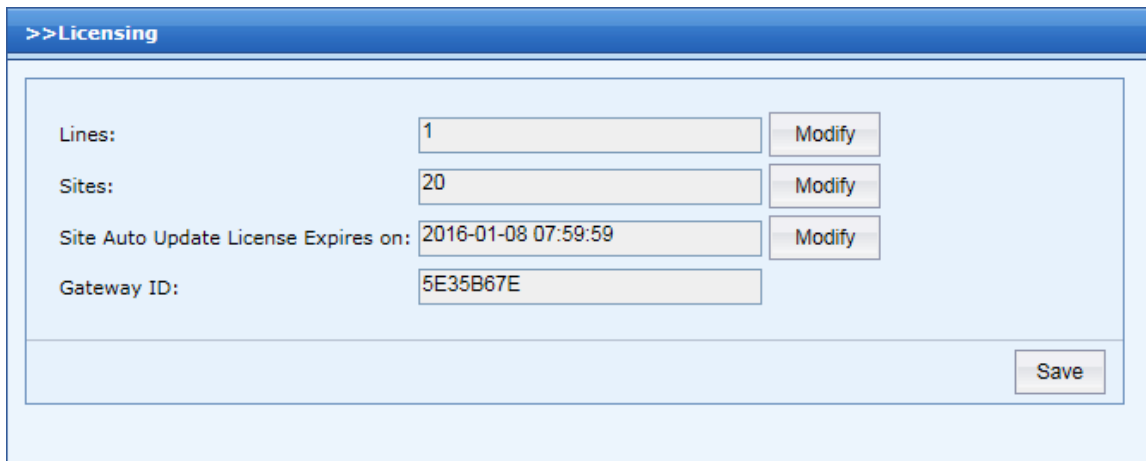
[System] include [Basics], [Network], [NGAF Central Mgt], [Administrators], [Database Management], [Advanced], [Firewall], [Backup/Restore], [Email Alarm Options], [Email Alarm Service], [Auto Update Server] and [Time Deviation Reminder] functions modules.

4.3.1. Basics

[Basics] include [Licensing], [WebAgent] and [System Time] function modules.

4.3.1.1 Licensing

[Licensing] is used to control CMC's lines and sites amount, sites auto-update expiry date as shown in the figure below:



Lines:	1	Modify
Sites:	20	Modify
Site Auto Update License Expires on:	2016-01-08 07:59:59	Modify
Gateway ID:	5E35B67E	

Save

[Lines] : The amount of WAN interface can be connected to CMC device.

[Sites] : The number of sites that can be connected to CMC device.

[Site Auto Update License Expires on] : CMC auto-update sites service expiry date.

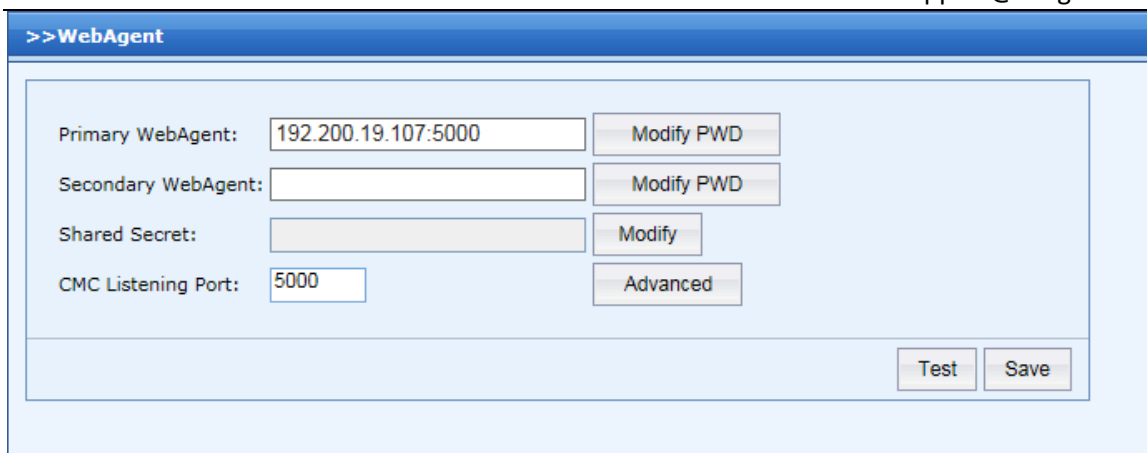
[Gateway ID] : The unique ID for each CMC device, not changable.



Mobile users and device gateway need authorization to connect to CMC device.

4.3.1.2 WebAgent

[WebAgent] is used to configure CMC's web agent address which include primary and secondary web agent, shared key and listening port, the page is shown as below:



The WebAgent configuration window has a blue title bar with the text ">>WebAgent". Inside, there are four rows of configuration fields:

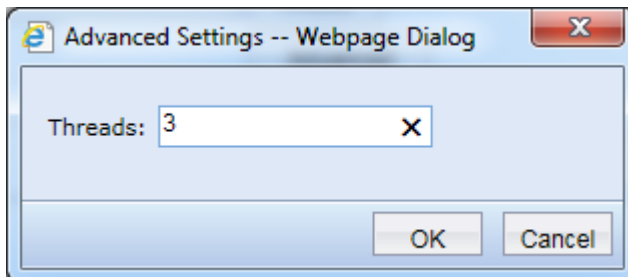
- Primary WebAgent: 192.200.19.107:5000 (with a Modify PWD button)
- Secondary WebAgent: (empty) (with a Modify PWD button)
- Shared Secret: (empty) (with a Modify button)
- CMC Listening Port: 5000 (with an Advanced button)

At the bottom right, there are Test and Save buttons.

If the web agent address is dynamic IP address, kindly insert web agent webpage address (usually end with .php extension). After fill in the web agent, users can click on **Test** to check the validity of the address. Meanwhile if the web agent address is static IP, kindly fill in web agent address with "IP address:port" format, for example 202.96.122.23:5000. Click on **Modify PWD** to configure password for web agent to prevent misuse purpose but this only works for webpage address. Click on **Modify** to configure shared key to prevent unauthorized access.

[CMC Listening Port] : This port is used by NGAF to connect to CMC, the port can be modified to another port number, however, need to ensure that the port used by NGAF is same with CMC.

[Advanced] : CMC's threads number as shown in the page below:



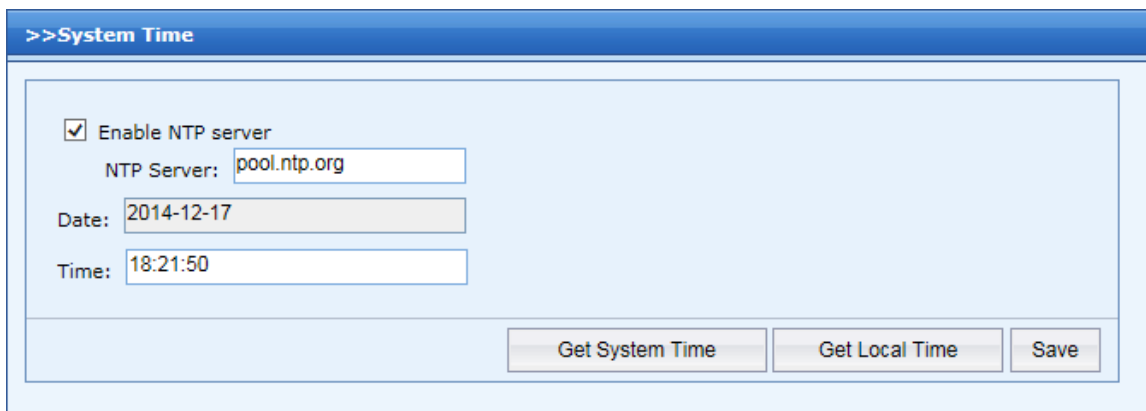
The Advanced Settings -- Webpage Dialog window has a title bar with a close button (X). Inside, there is a label "Threads:" followed by a text box containing the number "3" and a small X button. At the bottom, there are OK and Cancel buttons.



Warning : The maximum threads number can be configured in CMC is calculated as: Each threads can receive up to 1024 socket, each NGAF connecting to CMC need 2 sockets for single line connection; If both devices are using multiline socket number = line number of CMC x line number of NGAF x 2. Configure the number of threads based on the calculation to prevent waste of resources.

4.3.1.3 System Time

[System Time] is used to configure CMC system time, date and NTP server. The page is shown as below:



[Enable NTP Server] : After enabled this option, CMC will synchronize with NTP server for the date and time.

[Date] : Current CMC date

[Time] : Current CMC Time

Get System Time : Click to refresh the current page time.

Get Local Time : Set the CMC system time same to the PC system time which is used to log in to web console.

Click on **Save** to save the configuration.

4.3.2. Network

[Network] includes [Interface], [System Route] and [Multiple Lines] function modules.

4.3.2.1 Interface

[Interface] is used to configure CMC deployment and all interface's details such as IP address and etc. The page is shown below:

>>Interfaces

Deployment Mode

Mode: Gateway

Internal Interfaces

LAN Interface

IP Address: 11.254.254.254

Netmask: 255.255.255.0

DMZ Interface

IP Address: 10.254.253.254

Netmask: 255.255.255.0

WAN Interfaces

Line: Line1

☒ Enable this line

Line Type: Ethernet

☐ Obtain IP and DNS server using DHCP

IP Address: 192.200.19.107

Primary DNS: 8.8.8.8

Netmask: 255.255.255.0

Secondary DNS: 202.96.128.68

Line Selection Policy

Save

LAN Interface

IP Address: 11.254.254.254

Netmask: 255.255.255.0

DMZ Interface

IP Address: 10.254.253.254

Netmask: 255.255.255.0

WAN Interfaces

Line: Line1

☒ Enable this line

Line Type: Ethernet

☐ Obtain IP and DNS server using DHCP

IP Address: 192.200.19.107

Primary DNS: 8.8.8.8

Netmask: 255.255.255.0

Secondary DNS: 202.96.128.68

Default Gateway: 192.200.19.254

Multi-IP Binding

Line Selection Policy

Save

>>Interfaces

Deployment Mode
 Mode: Single Arm

Internal Interfaces

LAN Interface
 IP Address: 11.254.254.254
 Netmask: 255.255.255.0
 Default Gateway: 0.0.0.0

DMZ Interface
 IP Address: 10.254.253.254
 Netmask: 255.255.255.0

DNS Server
 Primary DNS: 0.0.0.0
 Secondary DNS: 0.0.0.0

Save

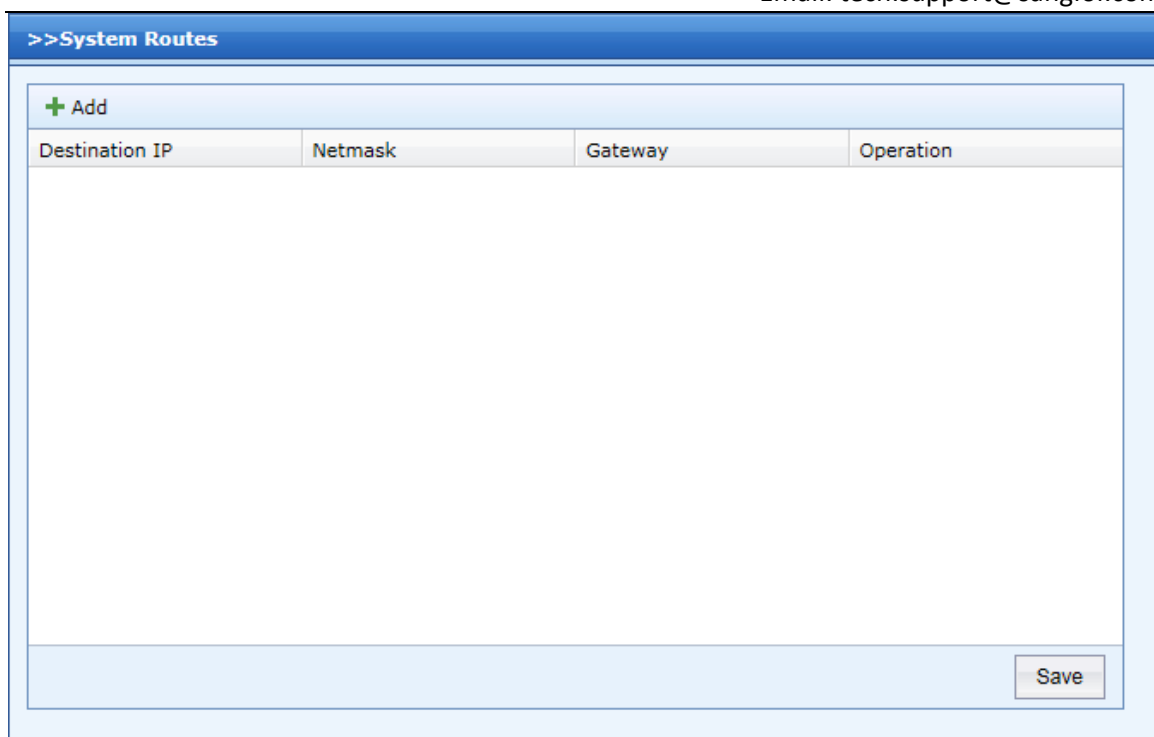
[Deployment Mode] : Includes Gateway mode and Single arm mode. Gateway mode indicates CMC device as gateway, Other than CMC related features, gateway mode CMC also include firewall, NAT and other functions. Single arm mode CMC need only a LAN interface for connection. CMC device online via NAT configuration on gateway device , this type of CMC has only basic CMC related features but not other features which available in gateway CMC.

[Internal Interface] : CMC's LAN and DMZ interfaces IP address and subnet mask configuration.

[WAN Interface] : Under Gateway mode deployment and is used to configure WAN interface related information such as lines type, IP address, subnet mask, default gateway and DNS.

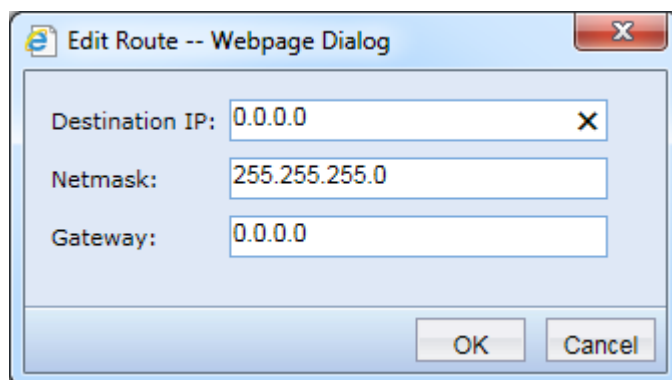
4.3.2.2 System Route

[System Route] is used to configure static route in CMC device, this feature is needed when there are remote networks in user's local network. The page is shown as below:



Destination IP	Netmask	Gateway	Operation
----------------	---------	---------	-----------

Click on **Add** button and the page in the figure below is shown:



Destination IP: 0.0.0.0 X

Netmask: 255.255.255.0

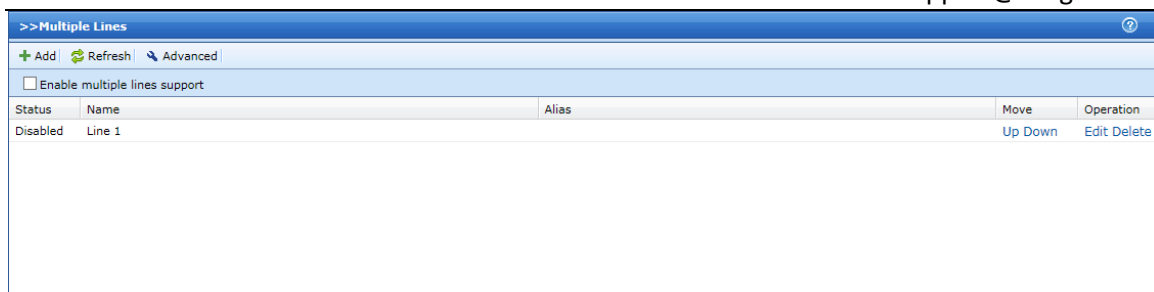
Gateway: 0.0.0.0

OK Cancel

Need to fill in related network address, subnet mask and gateway IP address and click **OK** to complete the configuration.

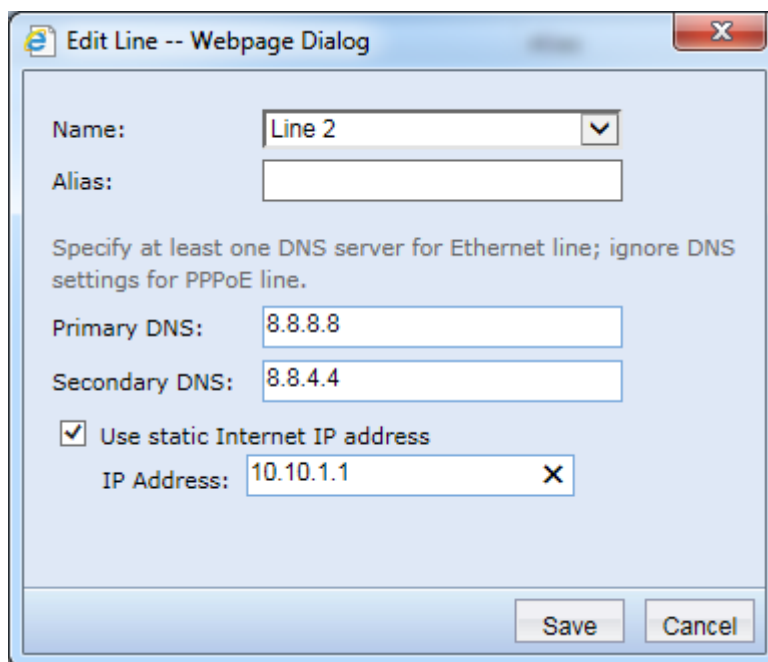
4.3.2.3 Multiple Lines

[Multiple Lines] is used during CMC gateway deployment mode and there are multiple lines connect to WAN interface, the page is shown below:



[Enable multiple lines support]: This option is used to enable/disable the multiple lines feature.

[Add] : Click on **Add** to create a new lines as shown in the figure below:



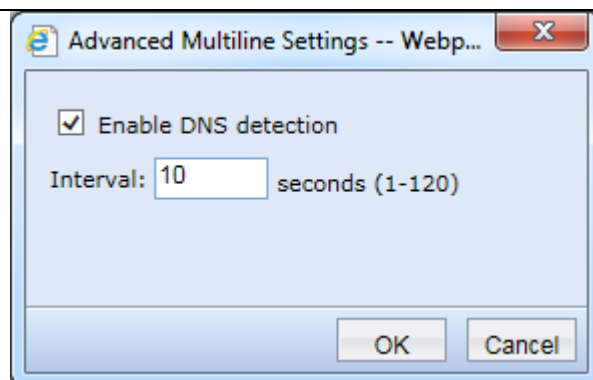
[Name] : Select on which line to used.

[Alias] : Self-define

[Primary DNS][Secondary DNS] : Fill in if public static IP address, if not just leave it blank.

[IP address] : Insert if the lines is using static public IP , else leave it blank.

[Advanced] : To determine whether enable/disable DMS detection, when DNS detection is enabled, the line will be treated as not functioning if not able to detect DNS. Click on the button and page below is shown:



Warning : If [lines type] is ethernet, DNS detection must be enabled and the DNS inserted must be valid. If ADSL dialup, DNS detection feature must be disabled.



Warning: After enable multiple lines support feature, the configuration under [multi line configuration] must be configure to use multiples lines.

4.3.3. NGAF Central Mgt

NGAF Central Mgt is used to manage rules database updates and auto-update status of internal datase.

4.3.3.1 Licensing

[Licensing] use to activate internal database rules which include Anti-virus, URL, IPS, Software update, application control, web application protection, and data leak protection databases;

>>Licensing

Gateway ID: 5E35B67E

Authorized Licensing: Activated Modify

Activated Module:

✓ Application Control	✓ Bandwidth Management	✓ VPN
✓ IPS	✓ Web Filter	✓ Anti-Virus
✓ APT Detection		

Internal Database Update licensing

Module	Expiry Date	Status	Operation
Anti-Virus Database	2015-12-10	Valid	Modify
URL Database	2015-12-10	Valid	Modify
Vulnerability Database	2015-12-10	Valid	Modify
Application Ident Database	2015-12-10	Valid	Modify
WAF Signature Database	2015-12-10	Valid	Modify
Data Leak Protection	2015-12-10	Valid	Modify
Malware Signature Database	2015-12-10	Valid	Modify

Save

[Internal Database Update licensing] shows all the database expiry date and the validity status. Click on Modify to change the license keys to validate the related database status.

4.3.3.2 Update Settings

Check on the [Enable sites download internal database from CMC] to allow NGAF device to download and update it's database via CMC but not via public.

>>Update Settings

☒ Enable sites download internal database from CMC

4.3.3.3 Update

[Update] page display current and latest NGAF internal database version details.

Click on **Update Now**, CMC will download related packages from official sites when CMC is able to access to internet.

Click on **Import** to upgrade the database to latest version manually.

>>Update

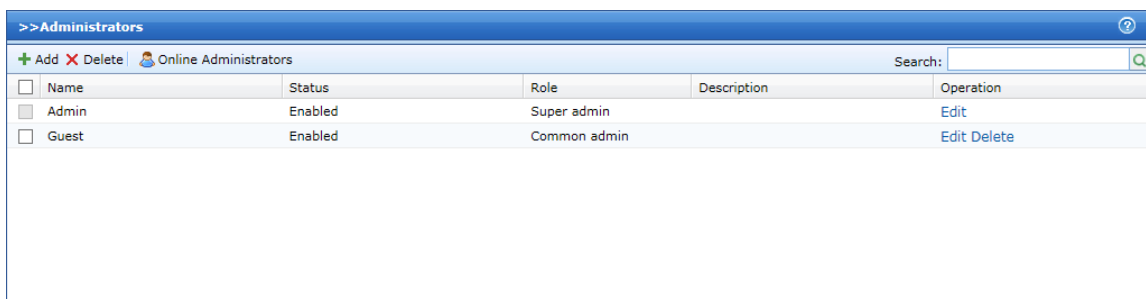
Refresh

Internal Database

Database	Current Version	Latest Version	Operation	
Anti-Virus Database	2014-10-20	2014-10-20	Update Now	Import
URL Database	2014-10-20	2014-10-20	Update Now	Import
Vulnerability Database	2014-10-17	2014-10-17	Update Now	Import
Software Update	*	Unknown version	Update Now	Import
Application Ident Database	2014-10-17	2014-10-17	Update Now	Import
WAF Signature Database	2014-10-17	2014-10-17	Update Now	Import
Data Leak Protection	2014-10-11	2014-10-11	Update Now	Import
Malware Signature Database	2013-05-13	Unknown version	Update Now	Import

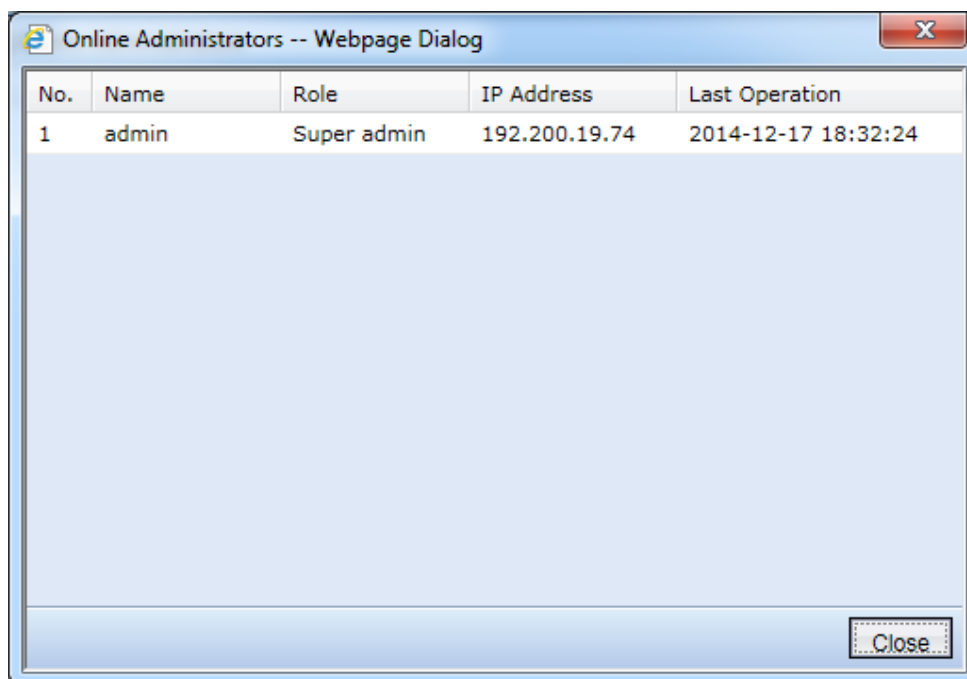
4.3.4. Administrators

[Administrators] page is used to configure CMC administrator account as shown below:



Name	Status	Role	Description	Operation
Admin	Enabled	Super admin		Edit
Guest	Enabled	Common admin		Edit Delete

[Online Administrators] : Can check on the admin who already logon to CMC device. The page below is displayed after click on the button.



No.	Name	Role	IP Address	Last Operation
1	admin	Super admin	192.200.19.74	2014-12-17 18:32:24

[Delete] : Click to delete selected administrator accounts, it will not affect unselected accounts.

[Add] : Add new administrator account, the page below is shown after click on **Add** button:



SANGFOR

SANGFOR Technologies Inc.

International Service Centre: +60 12711 7129 (7511)

Malaysia: 1700817071

Email: tech.support@sangfor.com

☒ Enable administrator☐ Free remote access to site

Basics

Name:

Role:

Common administrator

Password:

Confirm:

Description:

Authentication

☐ Hardware authentication

Certificate:

☐ Only allow login from the following IP

From:

To:

Valid Period

Realms

Save

Cancel



☒ Enable administrator ☐ Free remote access to site

password:

Confirm:

Description:

Authentication

☐ Hardware authentication
Certificate:

☐ Only allow login from the following IP
From: To:

Valid Period

Schedule:

☐ Account expires
On: : :

[Name], [Password], [Description] : Self-define/

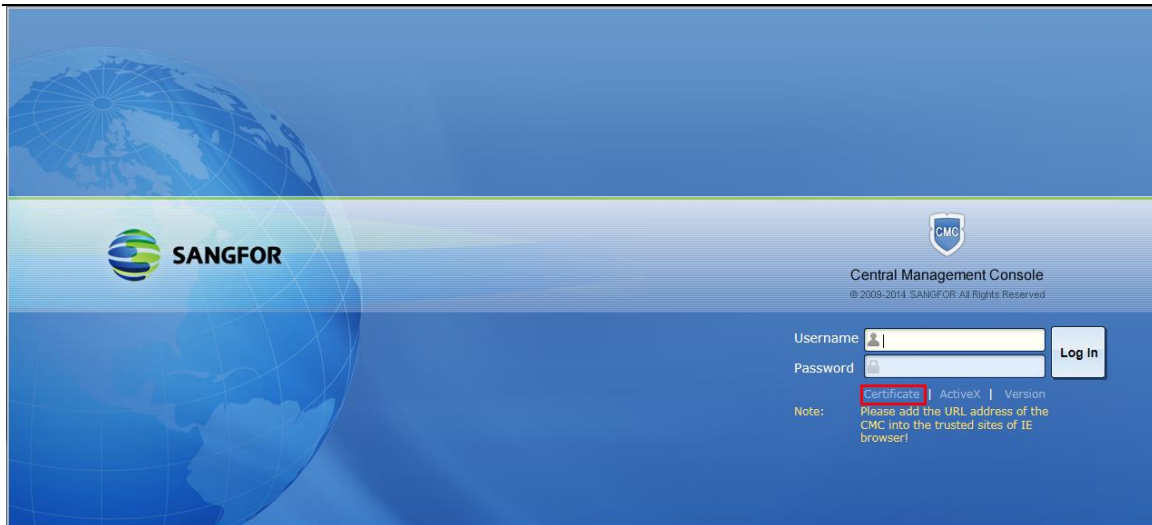
[Role] : There are 3 types : common administrator, group administrator and super administrator.

All of the roles have their own privilege which might be different from each and another.

[Hardware Authentication] : After enable this feature, when admin login to CMC web console, apart of inserting username and password, CMC device hardware certificate is needed also. If the certificate is different from certificate configured during account creation, the user will not be able to login to CMC web console.



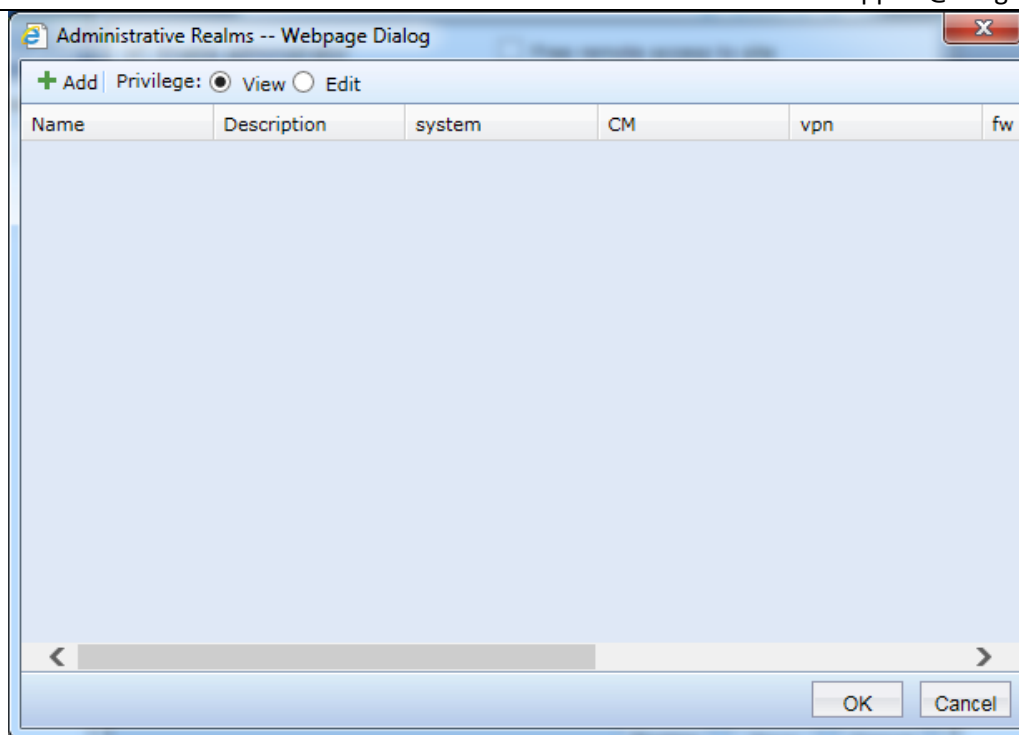
How to generate the hardware certificate? When user access CMC login page, there is a link connected to current hardware certificate as shown in the figure below:



[Only allow login from following IP] : When admin login to CMC web console, if the IP address of the PC using is not same with the IP address configured earlier in thi section, the user cannot access into CMC web console.

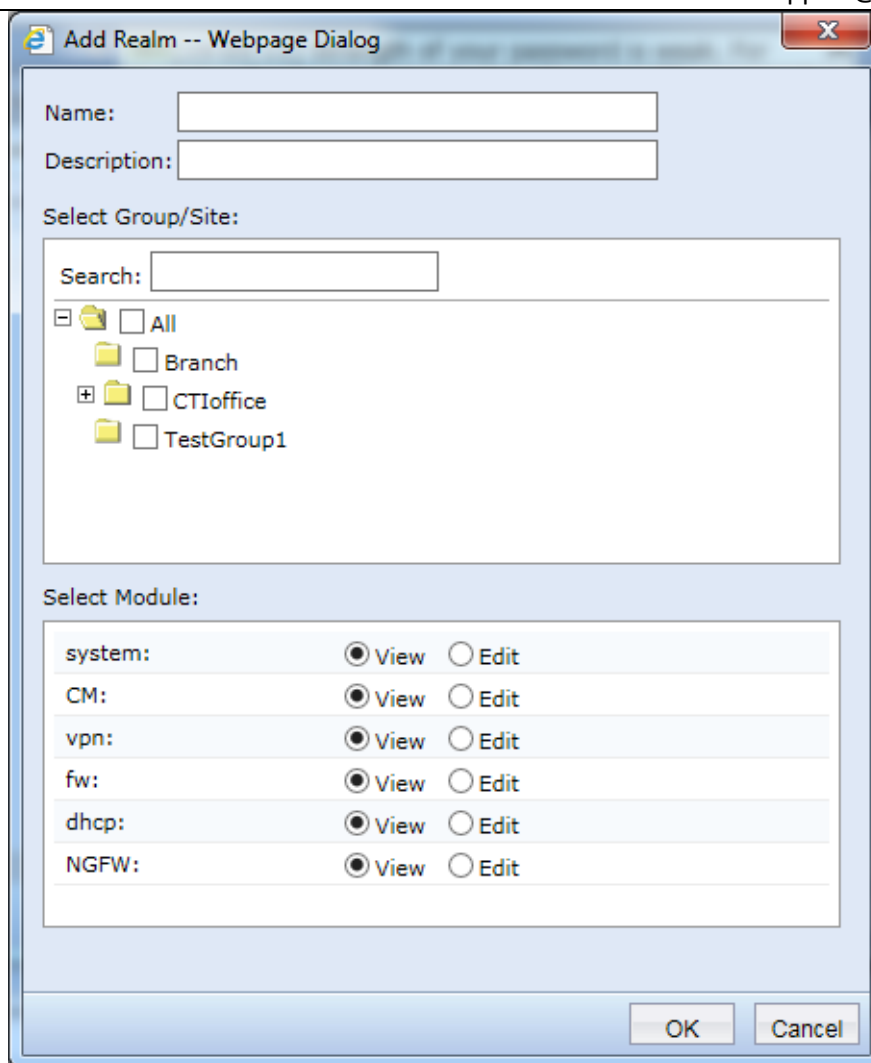
[Valid Period] : The valid period for administrator accounts created. If expired, user not able to access web console.

[Realms] : Admin user account privilege is configured here. If it is super administrator, the user account has super admin privilege which not able to be configured. If it is common administrator, click on **Realms** button and the page below is shown:



[Privilege] : Default is set to [View], can change to [Edit] manually.

Click on **Add** and the page below is prompted :



Add Realm -- Webpage Dialog

Name:

Description:

Select Group/Site:

Search:

- ☐ All
- ☐ Branch
- ☒ CTIoffice
- ☐ TestGroup1

Select Module:

system:	<input checked="" type="radio"/> View	<input type="radio"/> Edit
CM:	<input checked="" type="radio"/> View	<input type="radio"/> Edit
vpn:	<input checked="" type="radio"/> View	<input type="radio"/> Edit
fw:	<input checked="" type="radio"/> View	<input type="radio"/> Edit
dhcp:	<input checked="" type="radio"/> View	<input type="radio"/> Edit
NGFW:	<input checked="" type="radio"/> View	<input type="radio"/> Edit

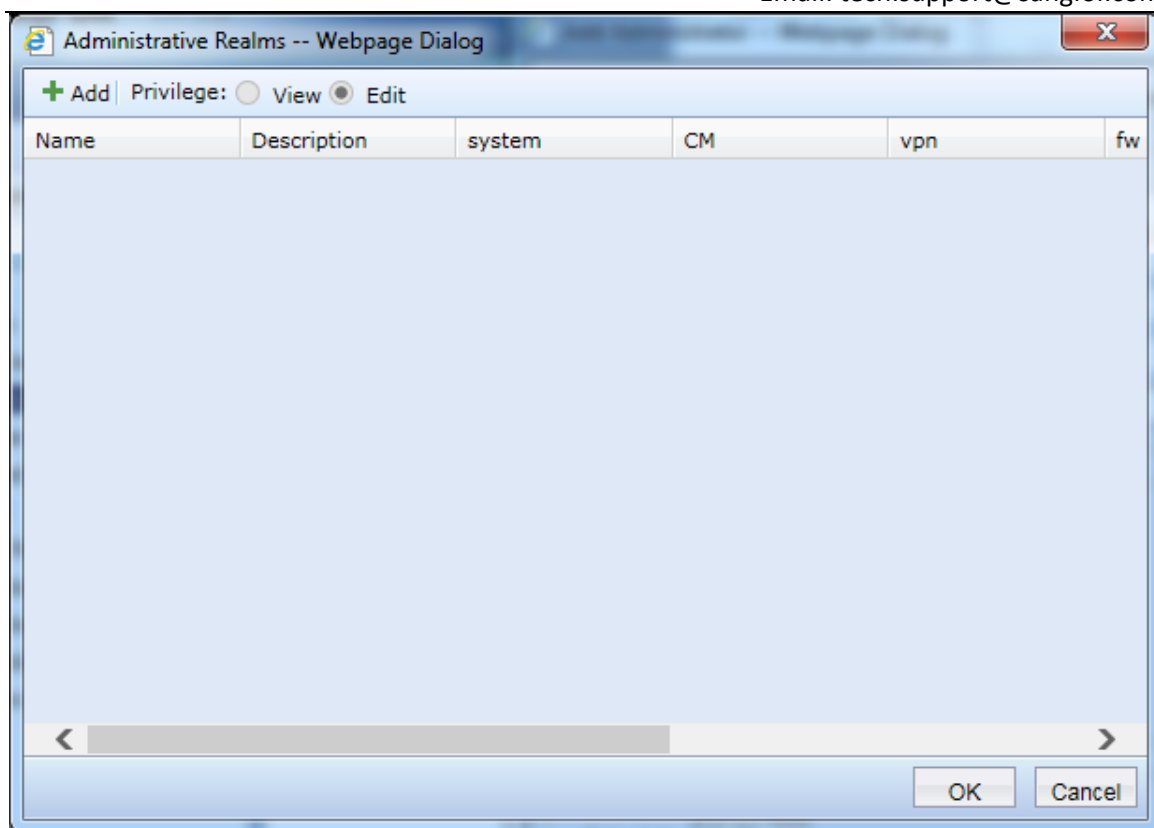
OK Cancel

[Name] and [Description] : Self-define.

[Select Group/Site] : Choose the Group/Site which to be managed by the current administrator user account.

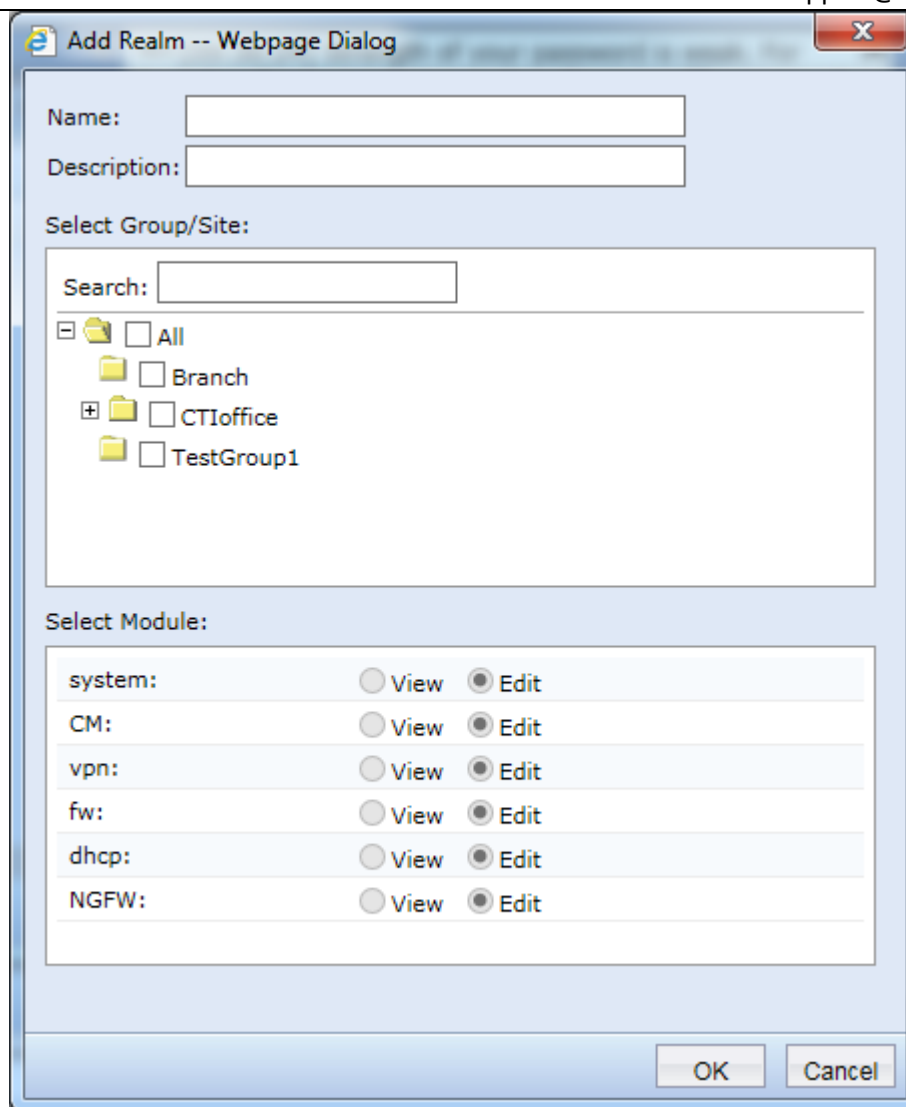
[Select Module] : Select the function modules which to be managed by the current administrator user account.

If the administrator user is group admin, click on **Realms** button and the page below is shown:



[Privilege] : Default is fixed to [Edit], can not be changed.

Click on **Add** and the page below is prompted :



Add Realm -- Webpage Dialog

Name:

Description:

Select Group/Site:

Search:

- ☐ All
- ☐ Branch
- ☒ CTIOffice
- ☐ TestGroup1

Select Module:

system:	<input type="radio"/> View	<input checked="" type="radio"/> Edit
CM:	<input type="radio"/> View	<input checked="" type="radio"/> Edit
vpn:	<input type="radio"/> View	<input checked="" type="radio"/> Edit
fw:	<input type="radio"/> View	<input checked="" type="radio"/> Edit
dhcp:	<input type="radio"/> View	<input checked="" type="radio"/> Edit
NGFW:	<input type="radio"/> View	<input checked="" type="radio"/> Edit

OK Cancel

[Name] and [Description] : Self-define.

[Select Group/Site] : Choose the Group/Site which to be managed by the current administrator user account.

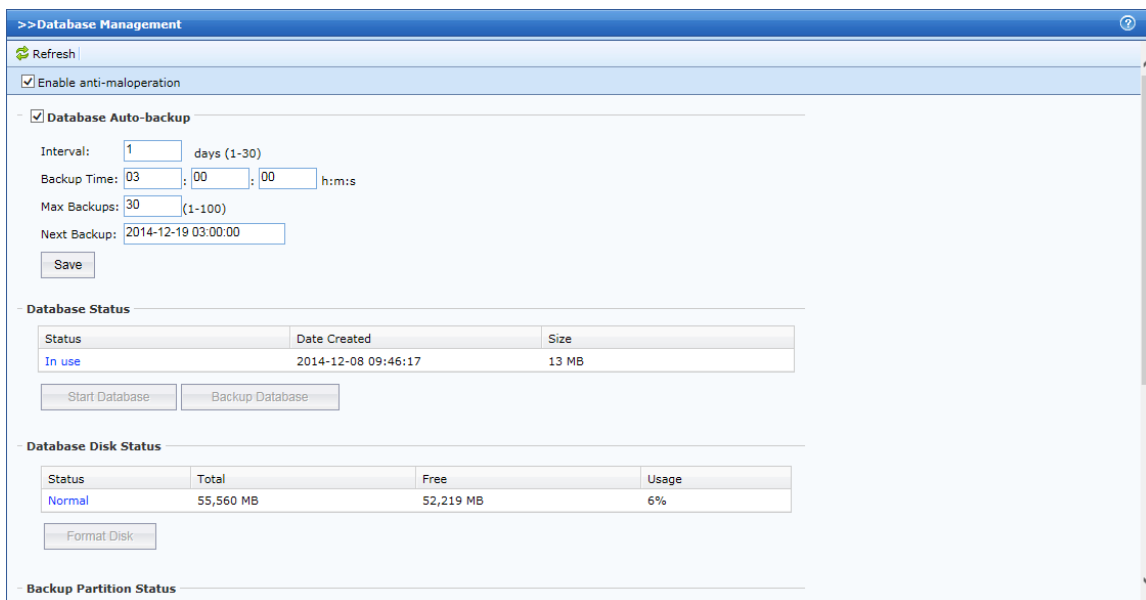
[Select Module] : Default is set to [Edit], cannot be modified.



Administrator user account cannot be deleted. Super admin can configure super administrator's user account, group administrator's user account and common administrator's user account. Group administrator's user account can modify group administrator's user account and common administrator's user account. Common administrator's user account can not create new administrator user account.

4.3.5. Database Management

[Database Management] is used to manage CMC's internal database, the page is shown below:



>>Database Management

Refresh

☒ Enable anti-maloperation

☒ Database Auto-backup

Interval: days (1-30)

Backup Time: : : h:m:s

Max Backups: (1-100)

Next Backup:

Save

Database Status

Status	Date Created	Size
In use	2014-12-08 09:46:17	13 MB

Start Database Backup Database

Database Disk Status

Status	Total	Free	Usage
Normal	55,560 MB	52,219 MB	6%

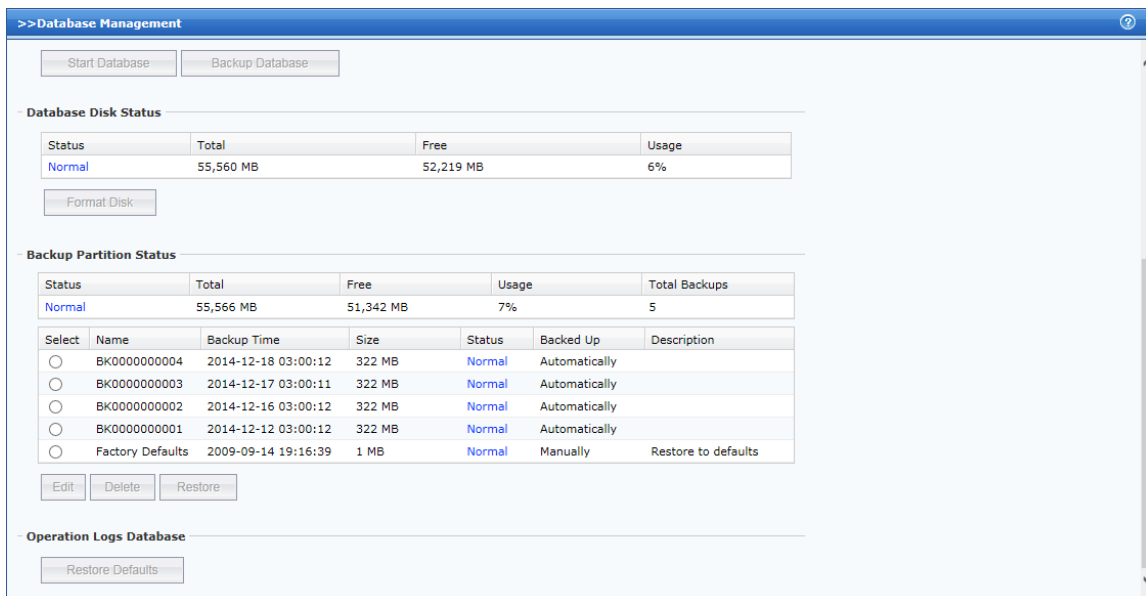
Format Disk

Backup Partition Status

[Enable Anti-maloperation] : Check this option to disable the configuration on this page, to prevent incorrect mis-configuration of the database.

[Database Auto Backup] : Can configure auto backup for CMC database base on day and time settings.

[Database Disk Status] : Display current CMC's internal storage usage status.



Start Database Backup Database

Database Disk Status

Status	Total	Free	Usage
Normal	55,560 MB	52,219 MB	6%

Format Disk

Backup Partition Status

Status	Total	Free	Usage	Total Backups
Normal	55,566 MB	51,342 MB	7%	5

Select	Name	Backup Time	Size	Status	Backed Up	Description
<input type="radio"/>	BK0000000004	2014-12-18 03:00:12	322 MB	Normal	Automatically	
<input type="radio"/>	BK0000000003	2014-12-17 03:00:11	322 MB	Normal	Automatically	
<input type="radio"/>	BK0000000002	2014-12-16 03:00:12	322 MB	Normal	Automatically	
<input type="radio"/>	BK0000000001	2014-12-12 03:00:12	322 MB	Normal	Automatically	
<input type="radio"/>	Factory Defaults	2009-09-14 19:16:39	1 MB	Normal	Manually	Restore to defaults

Edit Delete Restore

Operation Logs Database

Restore Defaults

[Backup Partition Status] : Select previous backup file or restore factory default backup, can also delete the backup file which is not using or cannot be used.

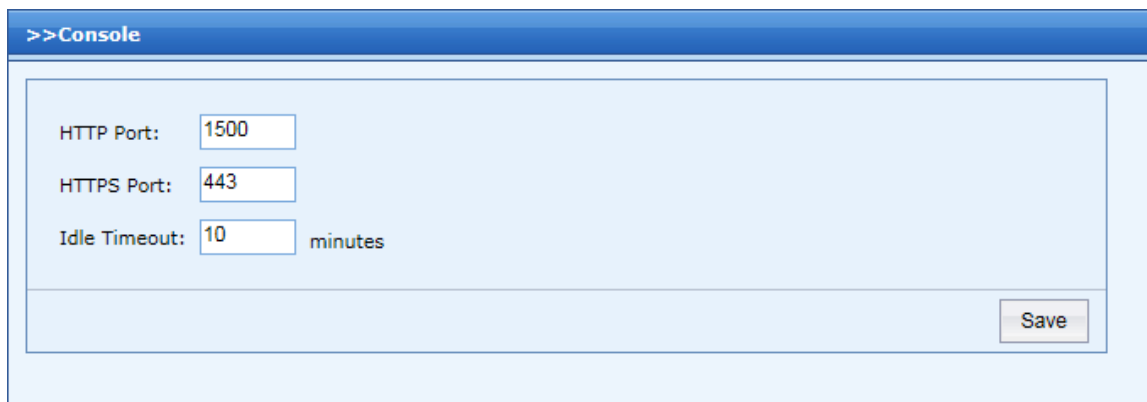
[Operation logs database] : Can restore operation log database to default.

4.3.6. Advanced

[Advanced] includes [Console], [Schedule], [Auto-update] and [LDAP Server] function modules.

4.3.6.1 Console

[Console] is used to configure CMC's web console login port and idle timeout period. The page is shown below:

The screenshot shows a web interface for configuring the console. At the top, there is a blue header bar with the text ">>Console". Below this, there is a light blue rectangular area containing three configuration items: "HTTP Port:" with a text box containing "1500", "HTTPS Port:" with a text box containing "443", and "Idle Timeout:" with a text box containing "10" followed by the word "minutes". At the bottom right of this area is a "Save" button.

[HTTP port] : Default is set to 1500. User can use http protocol with this port number to login to web console, the port number is changeable but can not conflict with CMC service port numbers.

[HTTPS port] : Default is set to 443. User can use https protocol with this port number to login to web console, the port number is changeable but can not conflict with CMC service port numbers.

[Idle Timeout] : Default is set to 10 minutes. CMC will automatically logout user if user idle for time period configured after logon to web console.

4.3.6.2 Schedule

[Schedule] is used to define commonly use time period and these defined schedule can be used in [Firewall] and [Access Control] to determine policy enable/disable time period. The schdule works base on CMC system time. The configuration page is shown below:



Click on **Add** button and the page below is shown:

For example, schedule “Working Hours” is configured, select the proper time period and then click on **Include** to indicates policy should be working in the selected period, click on **Save** to complete the configuration.

4.3.6.3 Auto-Update

[Auto-Update] module is used to configured whether CMC device should/should not download update package and perform auto-update. Check on [Enable system auto-update] to enable CMC device to perform update automatically once per day. By default, the auto-update interval time is set to 24 hours. The page is shown below:

>>Auto-update

☒ Enable system auto-update

With system auto-update enabled, updating will be performed automatically once per day.

Save

4.3.6.4 LDAP Server

[LDAP Server] is used as CMC's the third party authentication. The page is shown below:

>>LDAP Server

☒ Enable LDAP authentication

Server IP:

Port:

Admin DN:

Password:

Confirm:

Advanced Save

After done configuration on the page, click on **Advanced** and the page below will be displayed:

Server Type:	eDirectory
Search Filter:	ObjectClass=person
Logon Name Attribute:	cn
Root DN:	o=users,ou=sinfors,ou=com
Base DN:	o=users,ou=sinfors,ou=com
Timeout(s):	10
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

4.3.7. Firewall

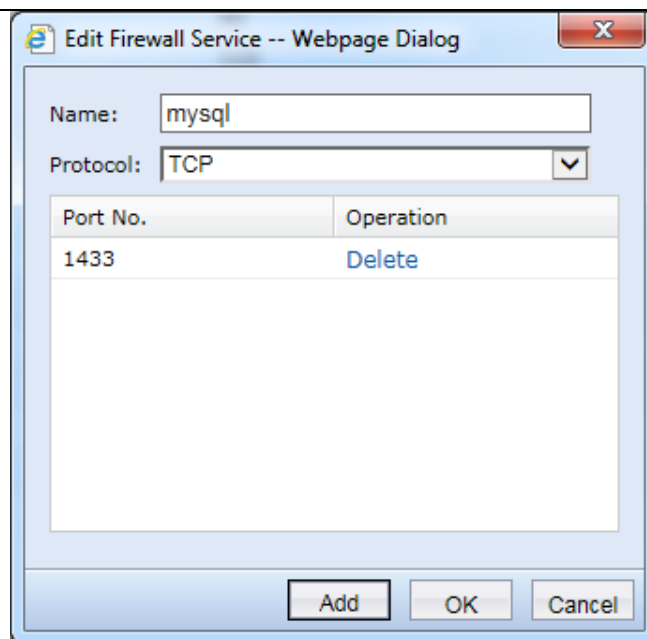
[Firewall] include [Services], [Firewall Rules] and [Anti-DoS] function modules. This feature works on traffics passing through CMC when deploy in gateway mode.

4.3.7.1 Services

Define the transport protocol and port in this section to identify the network operating software and communication program which using different transport protocol and ports via firewall rules. The page is shown below:

>>Services			
+ Add			
Name	Protocol	Details	Operation
http	TCP	80	Edit Delete
pop3	TCP	110	Edit Delete
smtp	TCP	25	Edit Delete
all-tcp	TCP	0-65535	Edit Delete
msn	TCP	1863	Edit Delete
ssl	TCP	443	Edit Delete
ftp	TCP	20-21	Edit Delete
ms-ds	TCP	445	Edit Delete
netmeeting	TCP	1503,1720	Edit Delete
anti-virus	TCP	135-139,445	Edit Delete
dns	UDP	53	Edit Delete
all-udp	UDP	0-65535	Edit Delete
ping	ICMP	type8 code0	Edit Delete

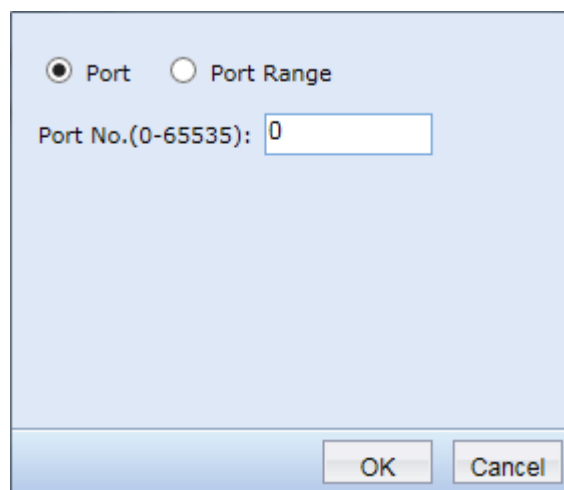
Click on **Add** button to define a service with specific transport protocol and port number as shown in the figure below:



[Name] : Self-define

[Protocol] : Select related protocol for the port, by default is TCP.

[Add] : Click on this button to add port/port range base on requirement, as shown in the figure below:

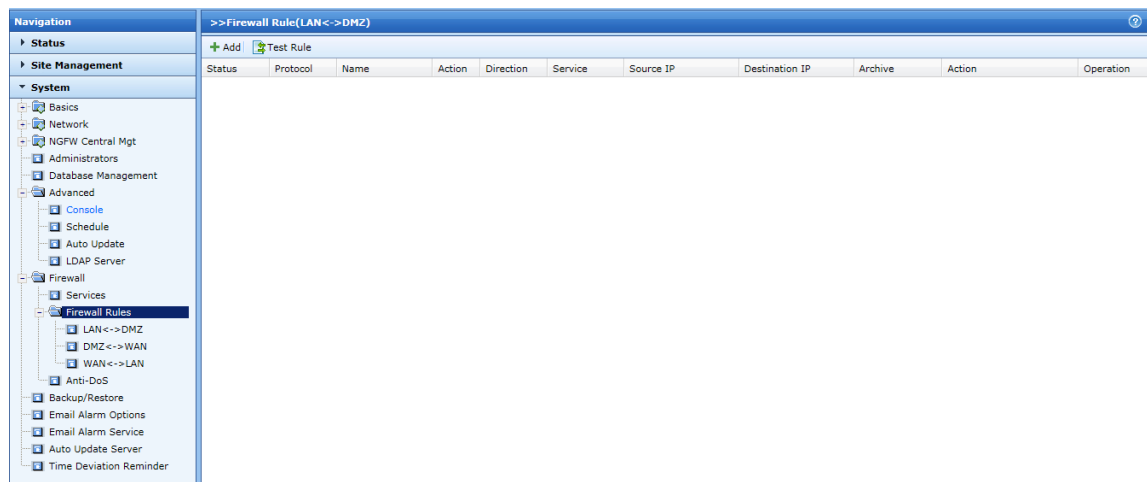


4.3.7.2 Firewall Rules

Sangfor CMC device's firewall uses packet state detection filtering technology, it can perform protocol, source and destination IP address packet filtering on multi direction forward and scheduling.

[Firewall Rules] include LAN<->DMZ, DMZ<->WAN and WAN<->LAN, 3 interfaces and 6

forwarding direction rules configuration. The page is shown below:



[LAN<->DMZ] : Is used to configure firewall rules between LAN interface and DMZ interface for both directions on CMC device.

[DMZ<->WAN] : Is used to configure firewall rules between DMZ interface and WAN interface for both directions on CMC device.

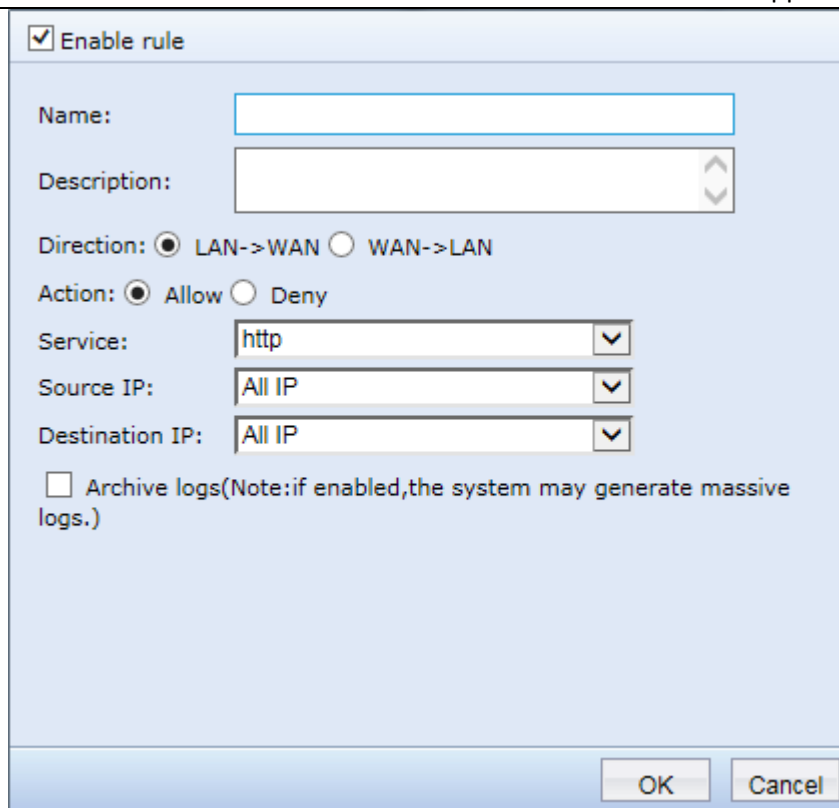
[WAN<->LAN] : Is used to configure firewall rules between WAN interface and LAN interface for both directions on CMC device.

Example below shows the firewall rules configuration between WAN<->LAN :

The figure below shows the configuration of firewall rules between WAN interface and LAN interface, it can be configured to allow or deny any services packets:

>>Firewall Rule(WAN<->LAN)										
Status	Protocol	Name	Action	Direction	Service	Source IP	Destination IP	Archive	Action	Operation
Enabled	TCP	anti-virus	Deny	LAN->WAN	anti-virus	All IP	All IP	Disabled	Move Up Move Down	Edit Delete
Enabled	TCP	all-tcp	Allow	LAN->WAN	all-tcp	All IP	All IP	Disabled	Move Up Move Down	Edit Delete
Enabled	UDP	all-udp	Allow	LAN->WAN	all-udp	All IP	All IP	Disabled	Move Up Move Down	Edit Delete
Enabled	ICMP	all-ping	Allow	LAN->WAN	ping	All IP	All IP	Disabled	Move Up Move Down	Edit Delete

Click on **Add** to define a new rules as follwing page:



[Name] : Self-define.

[Direction] : The rule will be applied based packet which direction match with the configuration.

[Action] : The action (Allow or Deny) to be taken on packets which match the condition.

[Service] : Service type to match packets.

[Source IP] : Source IP set to match on the packet's source IP address.

[Destination IP] : Destination IP set to match on the packet's destination IP address.

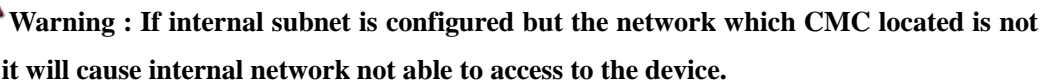
[Archive logs] : Check this option to log all the packets which match current firewall rule, normally this option is disabled in order to prevent massive logs generation on device.

4.3.7.3 Anti-DoS

This feature provide protection against denial of service (DoS) attacks from both internal and external network. DoS attack might cause bandwidth congestion or system hangs due to large amount traffics to be processed in a short time. Sangfor CMC is equipped with anti-DoS feature which can detect the amount of packets sent by each IP address, if the amount exceeds the amount allowed in CMC in specific period of time, CMC will assume the IP address performing DoS attack and will drop the related traffics for self-protection. The page is shown below:



Email: tech.support@sangfor.com



4.3.8. Backup/Restore

[Backup/Restore] is used to backup and restore CMC's interface's IP address, firewall module configuration but not include CMC database and administrator account configuration. The page is shown below:



The screenshot shows a web interface titled ">>Backup/Restore". It contains two main sections: "Backup Configuration:" and "Restore Configuration:". Under "Backup Configuration:", there is a "Backup" button. Under "Restore Configuration:", there is a "Browse..." button. Below these sections, there is a checkbox labeled "Backup reminder" which is checked, and a text input field labeled "Interval:" with the value "10" and the unit "days". A note at the bottom states: "Note: If ActiveX fails to run normally, please add the URL address of this device into trusted sites on your browser." A "Save" button is located at the bottom right of the form.

Click on **Backup** to backup CMC configuration. Click on **Browse**, then select the backup config file and click on **Save** to complete the restore process.

4.3.9. Email Alarm Options

[Email Alarm Options] is used to configured alarm event details and the alarm email settings such as recipient address. The page is shown below:

>>Email Alarm Options

Alarm-Triggering Events

☐ General alarm

☐ Site offline

☐ NGFW Site Alarm

☐ Site enables bypass

☐ Configuration distribution failure

Email Settings

Email Recipient:

Sending Interval: minutes (5-1440)

[Email Alarm Service](#)

By default, this page cannot be configured and is shown in grey color syntax because the [Email Alarm Service] has not been configured yet. To enable the configuration on this page, kindly configure the [Email Alarm Service] first by clicking on the blue color font. The page below is shown after clicking it :

>>Email Alarm Service

☒ Enable email alarm

Email Sender:

SMTP Server:

Test Email To:

☐ Require authentication

Username:

Password:

[Email Alarm Options](#)

After completed the configuration on [Email Alarm Service] page, kindly get back to the previous page as below:

>>Email Alarm Options

Alarm-Triggering Events

☐ General alarm

☐ Site offline

☐ NGFW Site Alarm

☐ Site enables bypass

☐ Configuration distribution failure

Email Settings

Email Recipient:

Sending Interval: minutes (5-1440)

[Email Alarm Service](#)

[General alarm] : Include sites disconnected issue.

[Site offline] : If a site's status from online turn to offline, then alarm email will be triggered.

[NGAF Site Alarm] : To enable [Site enables bypass] and [Configuration distribution failure] module detection.

[Sites enable bypass] : If a site 's bypass/enable packet drop function is turn on, alarm email will be sent to administrator.

[Configuration distribution failure] : If configuration yet distribute successfully to sites, alarm email will be triggered.

4.3.10. Email Alarm Service

[Email Alarm Service] is needed to enable alarm email function, to configure sender's email and mail server details. The page is shown below:



>>Email Alarm Service

☒ Enable email alarm

Email Sender:

SMTP Server:

Test Email To:

☒ Require authentication

Username:

Password:

[Email Alarm Options](#)

[Enable email alarm] : To enable this feature

[Email Sender] : Alarm email sender's address.

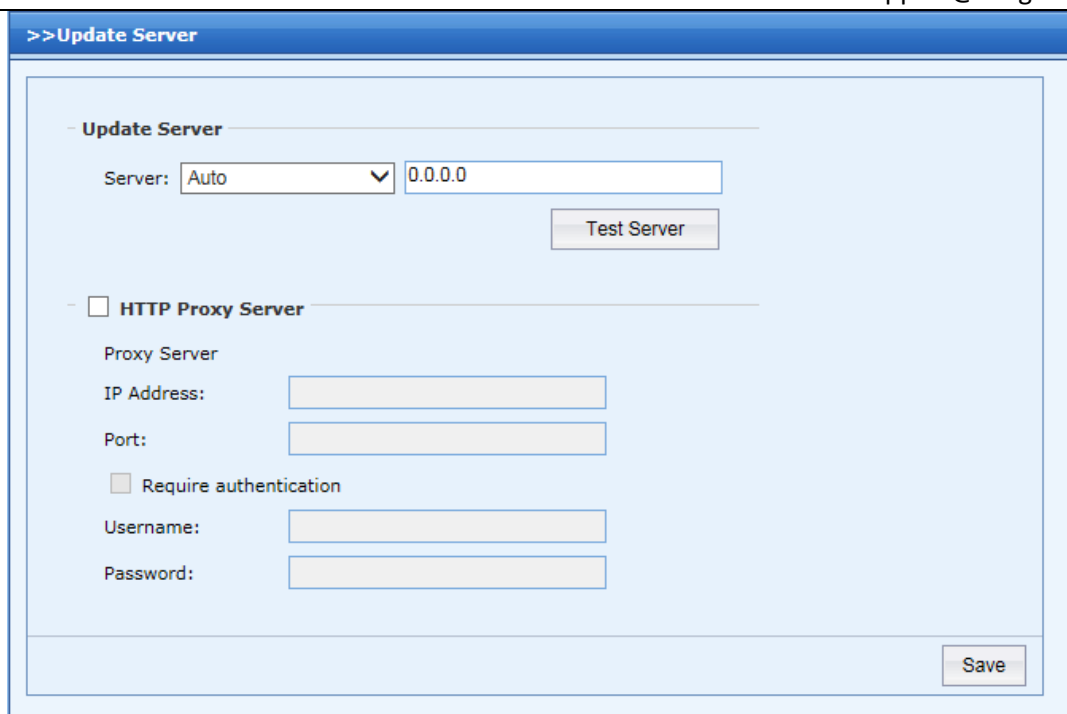
[Test Email To] : The test recipient's email address

[Require authentication] : To enable the settings for username and password of email server.

Click on **Send Test Email** to send validate the configuration.

4.3.11. Auto-Update Server

[Auto-Update Server] is used to configure the server which CMC connects to perform update for internal databases. The page is shown as below:

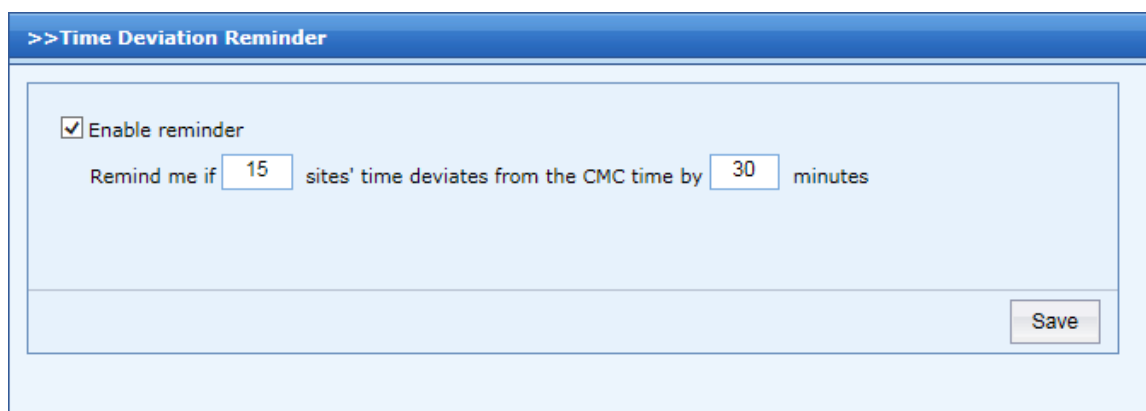


[Update Server] : Select the options available and click on **Test Server** to check on the availability of the server.

[HTTP Proxy Server] : CMC device update via a HTTP Proxy Server. Supports HTTP Proxy with authentication.

4.3.12. Time Deviation Reminder

[Time Deviation Reminder] configuration enable notice prompt message during administrator user login to web console if the number of sites which having time deviation issue exceed the limit. The page is shown below:





SANGFOR

SANGFOR Technologies Inc.

International Service Centre: +60 12711 7129 (7511)

Malaysia: 1700817071

Email: tech.support@sangfor.com

Select [Enable Reminder] to enable the function, fill in the number of sites and the time deviation.

Chapter 5 Sites Connecting

The Central Management Console (CMC) is designed to manage Sangfor NGAF devices distributed across a wide area network (WAN). With CMC, administrators can conveniently monitor and schedule update tasks for the NGAF devices with just a few clicks.

However, before the NGAF devices can be managed and monitored by the CMC, they must connect to the CMC. There are two key steps:

- 1 . Create sites on the CMC in Section 5.1
- 2 . Have the distributed NGAF devices connect to the CMC in Section 5.2

This chapter also discuss the common causes for configuration distribution failure and troubleshooting.

5.1. Creating Sites

By creating groups/sites, the CMC introduces the concept similar to groups/users and therefore conducts the hierarchical management. To have a NGAF device connect to the CMC, the corresponding site should be created on the CMC under a certain group which could be created based on geographical location or personal preferences.

Creating Groups/Sites

Log into the administrator console of the CMC and go to the Site Management > Groups/Sites page to create groups/sites, as shown below:

>>Groups/Sites

>>all Direct Sites: 3 Direct Groups: 1 Total Sites: 3

+ Add - Delete Configure Distribute Filter Advanced Search:

	Status	Device Model	Version	Subgroups	Description	Operation
Site	-	-	-	0		Config * Edit Distribute
Group	Enabled	NGFW-Device	NGFW 5.3	-		Config Edit Clone Distribute
Import site	Enabled	NGFW-Device	NGFW 5.3	-		Config Edit Clone Distribute
Auto-generate site	Enabled	NGFW-Device	NGFW 5.3	-		Config Edit Clone Distribute
test	Enabled	NGFW-Device	NGFW 5.3	-		Config Edit Clone Distribute

Page 1 / 1 Show page 1/1 Total 4 entries

Adding a Group

1. Click Add > Group to open the Add Group page, as shown below:

Name:

Description:

2. Enter the group name and description.
3. Click Save to apply the settings.

Adding a site

1. Click Add > Site to open the Add Site page, as shown below:

Device Series

Device Series:

Version:

2. Select device series and version.
3. Specify basic settings for the site.



Basic Information

☒ Enable site

☐ Use its own VPN configurations

Site Name:

Password:

Confirm:

Description: X

Group:

Device Model: ▼

Authentication: ▼

Back Next Cancel

4. The basic settings include site name, description, password, the group that the site belongs to, device model and authentication, as described in the following:

- Enable site

Check it to enable the site so that the corresponding NGAF can connect to the CMC; if it is unchecked, the corresponding device cannot connect to the CMC.

- Use its own configuration

If it's checked, when the site connects to the CMC, local configuration of VPN module will be uploaded to the site of the CMC. If it's unchecked, VPN module can be configured by the site of CMC. Then distribute the configurations to NGAF devices.

- Site Name

Specify a name for the site, which will be the username for the physical device to connect to the CMC.

- Password, Confirm

- Specify a password for the site, which will be the password for the physical device to connect to the CMC.

- Group

Select a group that the site belongs to. You can select the root group (that is, all) or a specific group (for example, group a).

- Device Model

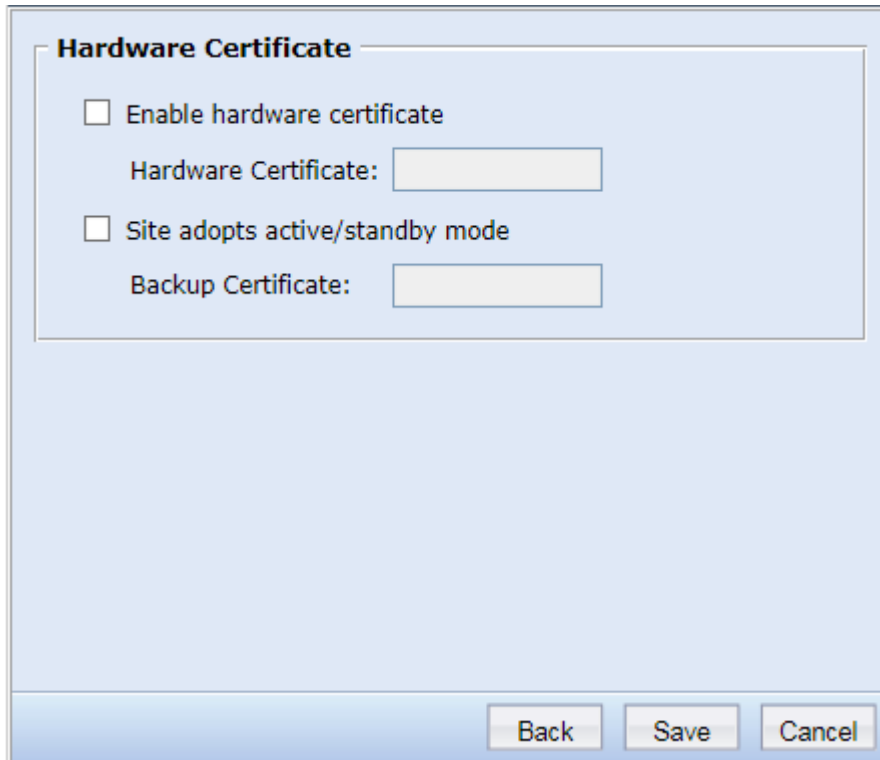
Select NGAF-Device which indicates the sangfor NGAF device.

- Authentication

Select an authentication mode, including local, LDAP, Radius server authentication.

5. Click Save to apply the settings.

6. Click Next to enter Hardware Certificate page, as shown below:



Enable hardware certificate: if checked, the certificate generated on the NGAF device can be imported onto the site. Once the certificate imported, the NGAF device will be tied with this site, as their certificates are the same. Therefore, the other NGAF devices cannot connect to the CMC through this site, as their certificates are not the same.

Site adopts active/standby mode: It's designed for the NGAF devices deployed in active/standby mode. As each device has its own hardware certificate, when the active device changes to standby state, it will cause the standby device cannot join CMC, because the certificates of standby device and the site are not the same. Therefore, you should also import the hardware certificate of standby device to ensure the standby device can join CM when HA failover occurs.

Import site

The pages of importing site and adding site are the same, the difference is that user can import the

sites by clicking Browse to select corresponding file.



Notes: Sites to being imported support .txt and .csv (each row format is the same. More than one records have multiple rows.). txt format: site name, password, csv format: site name, empty column, password

Auto-generate site

The difference between the pages of auto-generate site and adding site is that there are additional fields on the auto-generated page: name prefix and number of sites. For example, enter NGAF in Name Prefix field and 100 in Number of sites field, and click Save. Then 100 sites will be generated automatically.

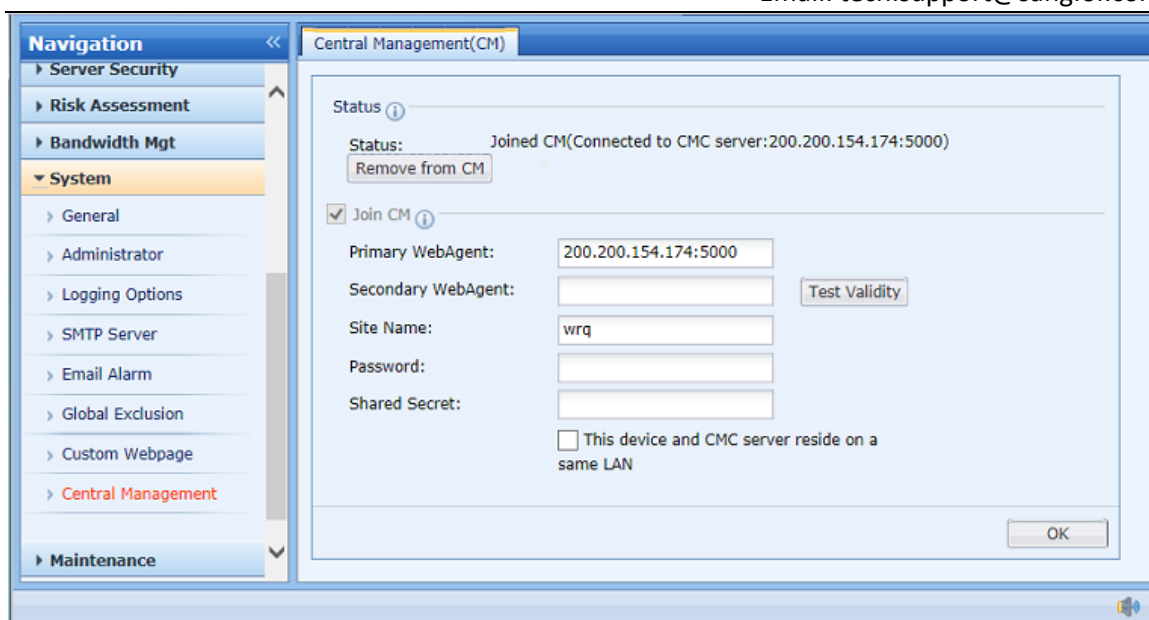
5.2. Connecting to the CMC

Sites indicate Sangfor NGAF devices that can be centrally managed and monitored by the Sangfor Central Management Console (CMC) after they connect to the CMC. To have a NGAF device successfully connect to the CMC, create the site on the CMC and configure the CMC connection options on the NGAF device.

Site Connecting to the CMC

To have a site connect to the CMC,

1. Log into the administrator console of the CMC and create the site (see Creating Sites).
2. Log into the administrator console of the site (NGAF) and go to the System > Central Management page, as shown below:



3. Specify the following information.

- Primary WebAgent

Enter the WebAgent address in format of IP:Port or URL. The WebAgent will be used by the site to obtain the network location of the CMC, and therefore it should be the physical IP address or domain name (if available) of the CMC. If the CMC is assigned a WebAgent address by the manufacturer, enter the corresponding URL address.

- Test WebAgent

Click it to test the connectivity between the site and CMC. Please note that this button does not work when the WebAgent address is a URL address.

- Secondary WebAgent

Secondary WebAgent indicates the standby WebAgent address which will be used by the site to connect to the CMC when the primary WebAgent is unavailable.

- Site Name

Enter the username for connecting to the CMC. It should be the name of the corresponding site created on the CMC.

- Password

Enter the password for connecting to the CMC. It should be the password of the corresponding site created on the CMC.

- Shared Secret

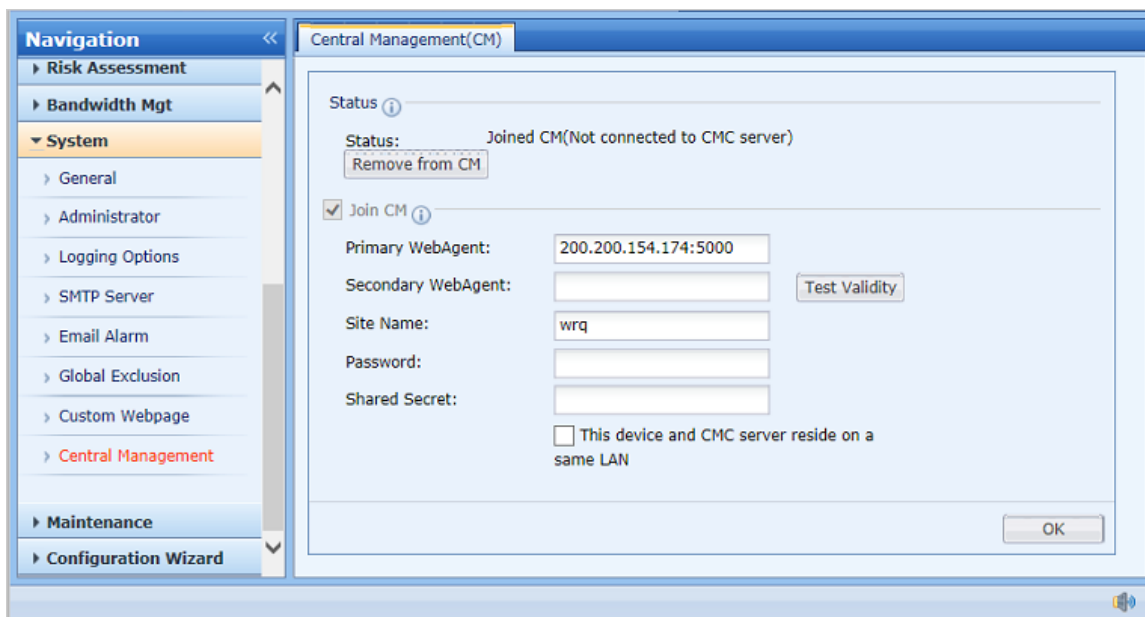
Enter the shared secret which should be the same as that configured on the CMC. Ignore it if no shared secret is set on the CMC.

- This device and CMC server reside on a same LAN

Specify whether the CMC resides on the same local area network as the NGAF.

After clicking OK, you should login again.

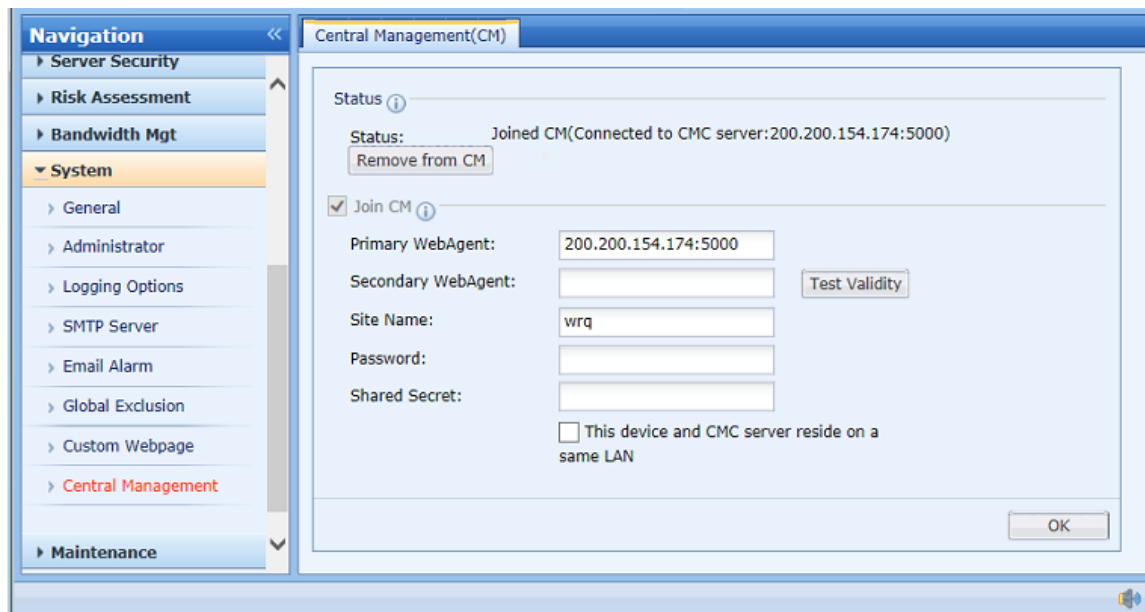
If the site has joined CM, but it does not connect to the CMC, as shown below:



The screenshot shows the 'Central Management(CM)' configuration window. On the left is a 'Navigation' pane with categories: Risk Assessment, Bandwidth Mgt, System (selected), Maintenance, and Configuration Wizard. Under 'System', options include General, Administrator, Logging Options, SMTP Server, Email Alarm, Global Exclusion, Custom Webpage, and Central Management (highlighted in red). The main panel shows the 'Status' as 'Joined CM(Not connected to CMC server)' with a 'Remove from CM' button. Below this, the 'Join CM' checkbox is checked. Fields for 'Primary WebAgent' (200.200.154.174:5000), 'Secondary WebAgent', 'Site Name' (wrq), 'Password', and 'Shared Secret' are present, along with a 'Test Validity' button. At the bottom, there is an unchecked checkbox labeled 'This device and CMC server reside on a same LAN' and an 'OK' button.

Please check if the site name, password and shared secret are identical with the site name, password and shared secret configured on the CMC. Otherwise, connecting to the CMC will fail.

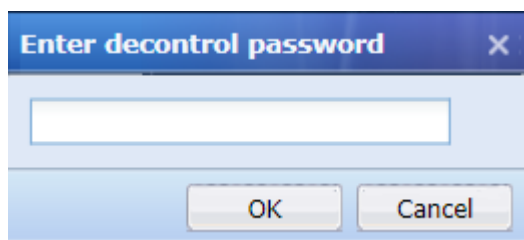
If the network connection is available and the site can join Central Management(CM) successfully, you can view the following figure:



This screenshot is similar to the previous one but shows a successful connection. The 'Status' is now 'Joined CM(Connected to CMC server:200.200.154.174:5000)'. The 'Join CM' checkbox remains checked, and the configuration fields (Primary WebAgent, Secondary WebAgent, Site Name, Password, Shared Secret, and Test Validity button) are identical. The 'This device and CMC server reside on a same LAN' checkbox is still unchecked, and the 'OK' button is at the bottom right.

Site Removed from CM

To remove a site from CM, go to the System > Central Management page, and click on Remove from CM. Then the following prompt pops up:



Enter correct decontrol password. Then the site can be removed from CM and will not be managed by the CMC any more.

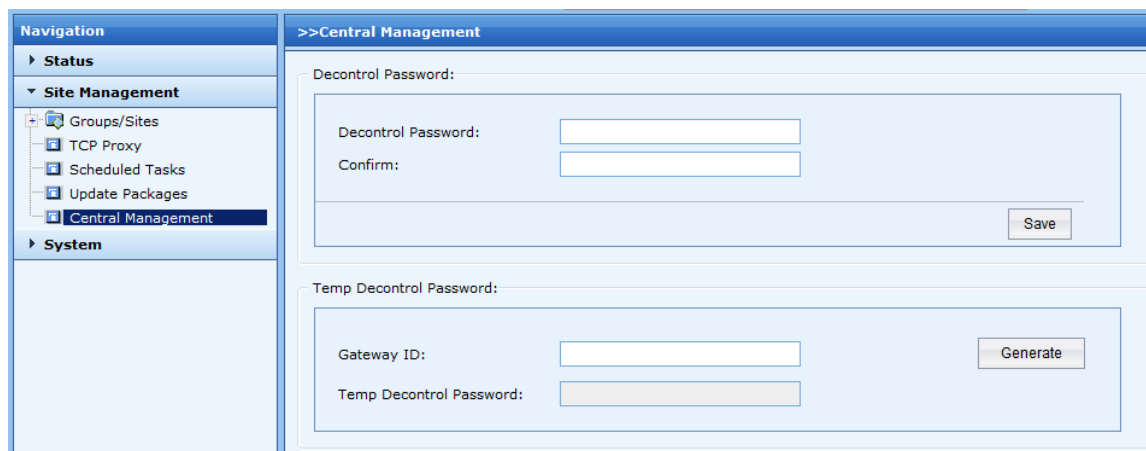
Decontrol password can be modified on the CMC, and can also be a temp one generated by the CMC, which will get expired after the day.

After the site is removed from the CM, it will login again automatically.

Decontrol Password

To modify decontrol password on the CMC,

1. Log into the administrator console of the CMC.
2. Go to Site Management>Central Management page, as shown below:



3. Enter decontrol password and confirm it. Click Save to save your settings.
4. Decontrol password will be distributed to the site automatically. It will be used when you want to remove the site from CM.

Generate Temp Decontrol Password

Enter gateway ID and click Generate. Then a temp decontrol password will be generated, which will get expired after the day. It will be used when you want to remove the site from CM.



The differences between the decontrol password and temp decontrol password are as follows:

1. Decontrol password should be dispatched to site by the CMC and will never get expired. It is applicable to all the sites.
2. Temp decontrol password is generated on the CMC. It should be sent to the administrator of site by email, SMS or telephone, and will get expired after the day.

5.3. Common Causes for Config Distribution Failure

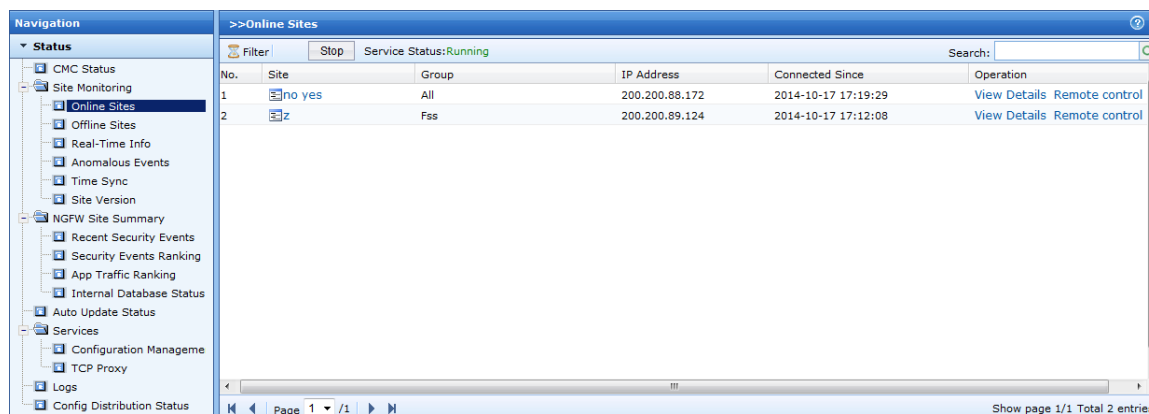
When configurations are dispatched to terminals by the CMC, if the terminals haven't received the configuration file, that means the CMC failed to dispatch the configurations. The failure reason is more than one. For how to find out the reasons, you can refer to the following methods:



Note: The following methods are applicable to the cases that common causes lead to configuration distribution failure, and do not include all the troubleshooting methods.

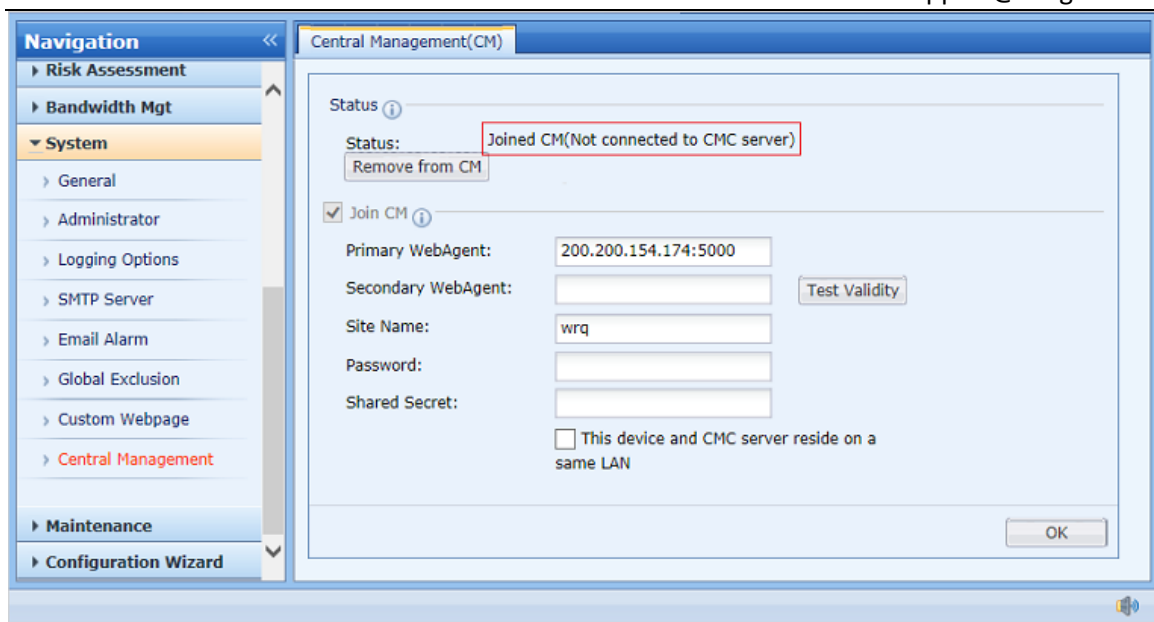
Check if the terminal connected to CMC

1. Log into CM console and go to Status > Site Monitoring > Online Sites page to check if the site is in the online site list. If the site connected to the CMC, corresponding site information will be displayed on this page, as shown below:



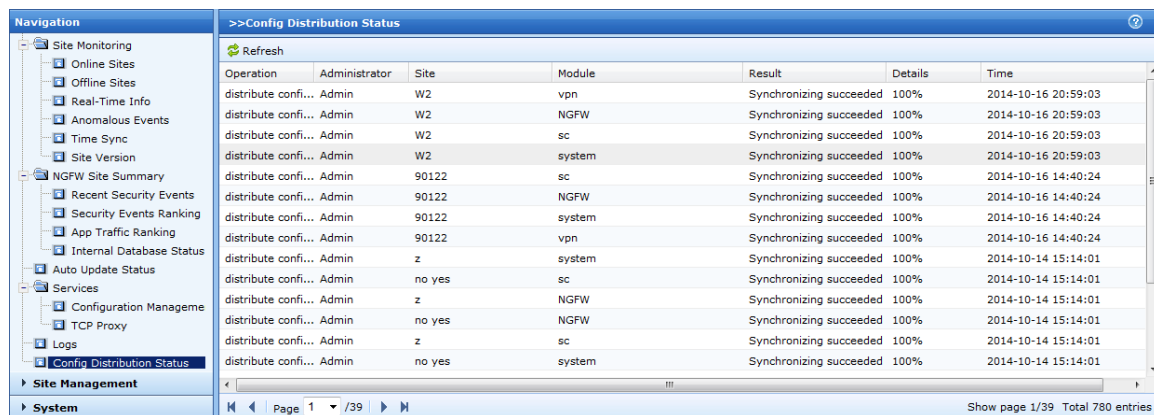
No.	Site	Group	IP Address	Connected Since	Operation
1	no yes	All	200.200.88.172	2014-10-17 17:19:29	View Details Remote control
2	z	Fss	200.200.89.124	2014-10-17 17:12:08	View Details Remote control

2. Log into NG Firewall console and go to System > Central Management page to check if the settings for joining CM is correct, as shown below:



View Config Distribution Logs on CMC

Go to Status > Services > Config Distribution Logs to check if the configuration is dispatched successfully. If success, 100% will be showed in Details column. Otherwise, 0% will be showed.



Operation	Administrator	Site	Module	Result	Details	Time
distribute confi...	Admin	W2	vpn	Synchronizing succeeded	100%	2014-10-16 20:59:03
distribute confi...	Admin	W2	NGFW	Synchronizing succeeded	100%	2014-10-16 20:59:03
distribute confi...	Admin	W2	sc	Synchronizing succeeded	100%	2014-10-16 20:59:03
distribute confi...	Admin	W2	system	Synchronizing succeeded	100%	2014-10-16 20:59:03
distribute confi...	Admin	90122	sc	Synchronizing succeeded	100%	2014-10-16 14:40:24
distribute confi...	Admin	90122	NGFW	Synchronizing succeeded	100%	2014-10-16 14:40:24
distribute confi...	Admin	90122	system	Synchronizing succeeded	100%	2014-10-16 14:40:24
distribute confi...	Admin	90122	vpn	Synchronizing succeeded	100%	2014-10-16 14:40:24
distribute confi...	Admin	z	system	Synchronizing succeeded	100%	2014-10-14 15:14:01
distribute confi...	Admin	no yes	sc	Synchronizing succeeded	100%	2014-10-14 15:14:01
distribute confi...	Admin	z	NGFW	Synchronizing succeeded	100%	2014-10-14 15:14:01
distribute confi...	Admin	no yes	NGFW	Synchronizing succeeded	100%	2014-10-14 15:14:01
distribute confi...	Admin	z	sc	Synchronizing succeeded	100%	2014-10-14 15:14:01
distribute confi...	Admin	no yes	system	Synchronizing succeeded	100%	2014-10-14 15:14:01

Check Sync Status

If the sync status of NGAF module displayed 0%, you can view anomalous status of sites on Status > Site Monitoring > Anomalous Events page. The information about inconsistent versions and number of entries exceeding upper limit after merging will be displayed.



If the above steps completed, the reasons cannot be found. Please contact Customer Service. We will provide technical support timely.