CMC 4.3 User Manual

Table of Contents

1.0 Introduction

Console Administration

- ### Login to Console

  Type the address "https://Device IP" in your browser (Device IP should be replaced by the IP address of the CMC) and then login to the administrator console.

  Please use the IE browser (IE 7 or above) to login, for some functions may require the ActiveX control to be installed. The IE 6 is not supported as its performance is relatively lower.

- ### To Make Settings Take Effect

  After configuring the options, click Save to apply the settings. A restart of CMC or the services may be required for some settings to take effect, in which case, a prompt will pop up.

- ### Getting Help
  1. Click the Help link in the upper-right corner of the administrator console to obtain the Help Document.
  2. Click the icon in the upper-right corner of each page.
  3. Move your mouse pointer over the checkboxes of some options to see the tips or brief description.

Getting More Help

- **Website:** http://www.sangfor.com
- **MSN, Email:** tech.support@sangfor.com.hk
- **Skype:** sangfor.tech.support
- **TEL:** + 60 3 2282 1206

2.0 Site Connecting

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

However, before the WOCs 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 (see Creating Sites).
2. Have the distributed WOCs connected to the CMC (see Connecting to the CMC).

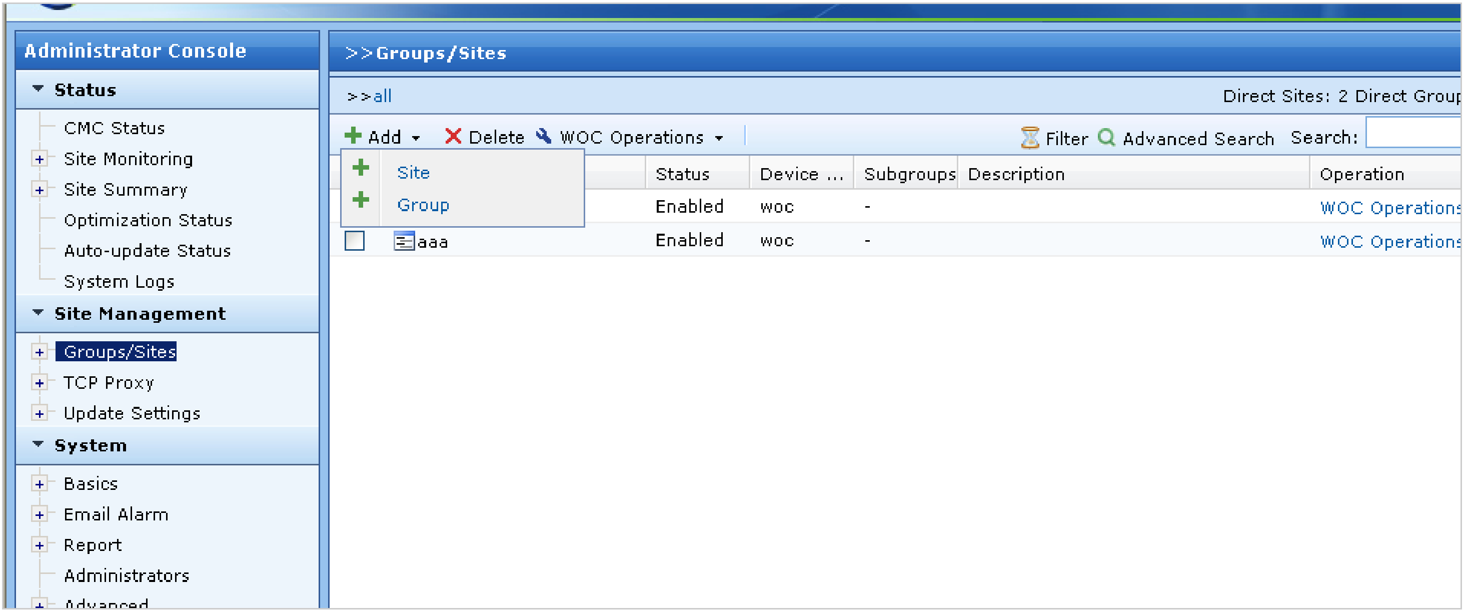
2.1 Creating Sites

Overview

By creating groups/sites, the CMC introduces the concept similar to groups/users and therefore conducts the hierarchical management. To have a physical WOC 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:



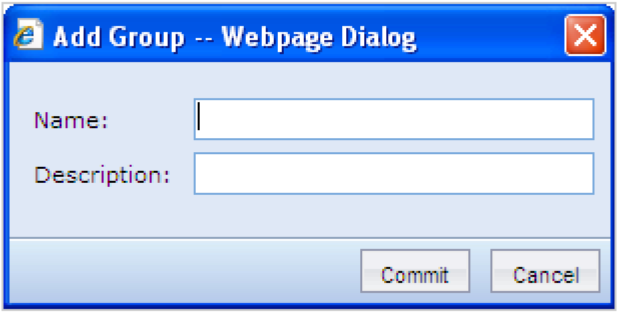
Direct Sites: 2 Direct Group

	Status	Device ...	Subgroups	Description	Operation
	Enabled	woc	-		WOC Operations
□ aaa	Enabled	woc	-		WOC Operations

For the relationship between a group and its subgroups/sites, see Hierarchical Organization.

Adding a Group

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



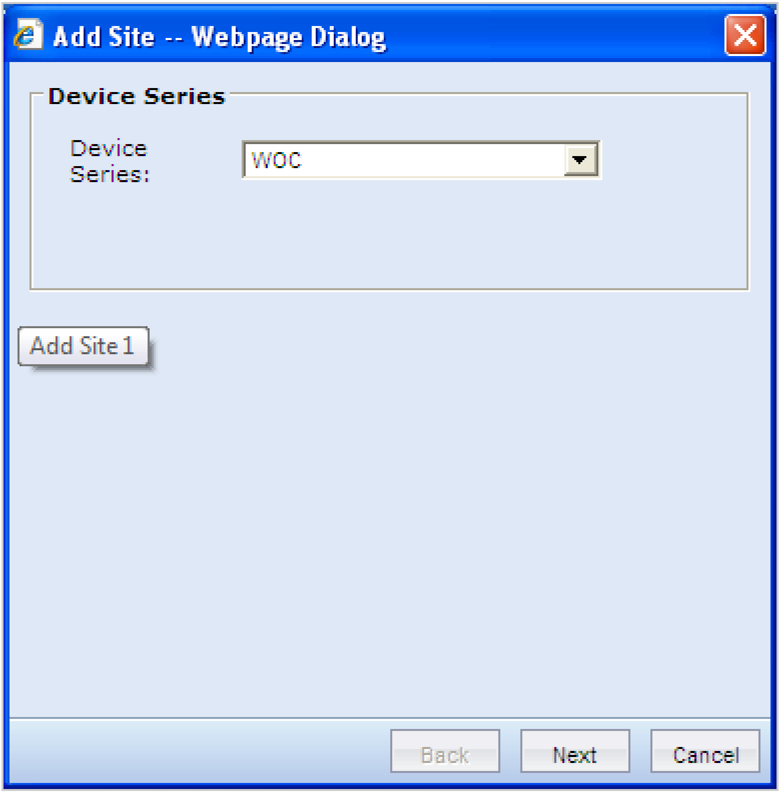
Name:

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:

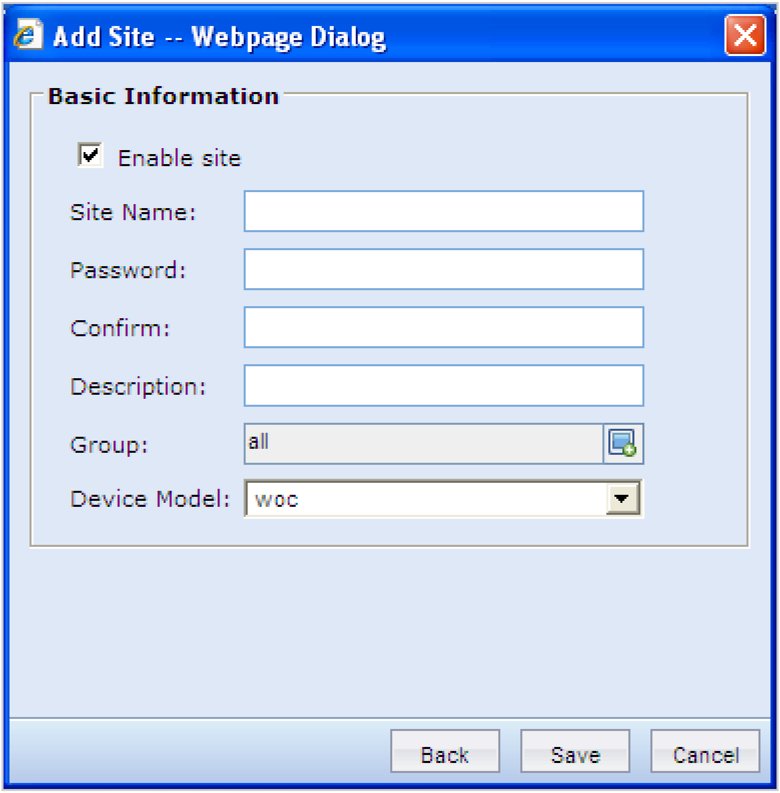


Add Site -- Webpage Dialog

Device Series

Device Series: WOC

2. Select the device type.
3. Specify the basic settings for the site.



Add Site -- Webpage Dialog

Basic Information

☑ Enable site

Site Name:

Password:

Confirm:

Description:

Group: all

Device Model: woc

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 WOC can connect to the CMC; if it is unchecked, the corresponding device cannot connect to the CMC.

- **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 WOC which indicates the Sangfor WAN Optimization Controller.

4. Click Save to apply the settings.

2.2 Connecting to the CMC

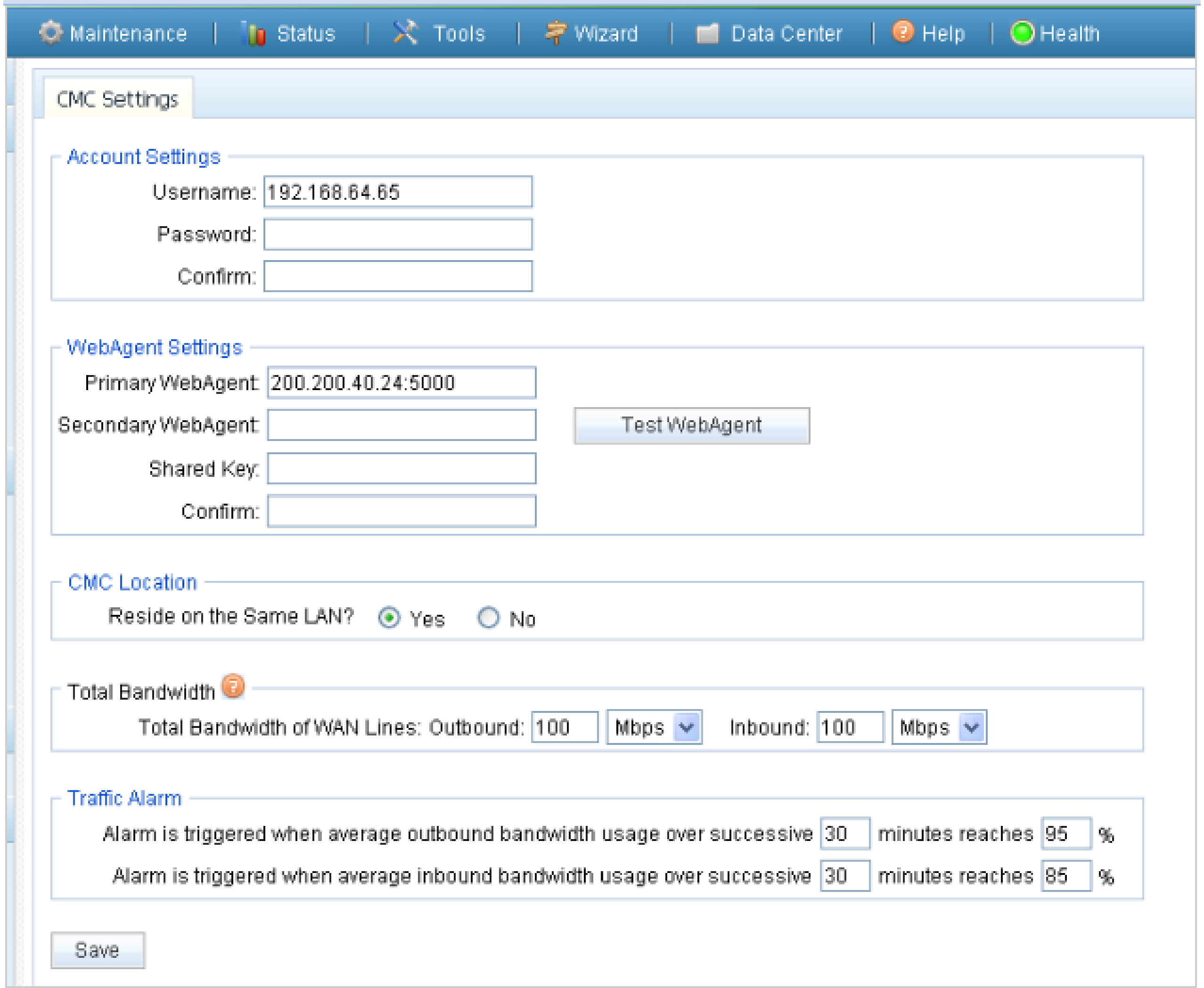
Overview

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

Sites 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 (WOC) and go to the System > CMC Connection page, as shown below:



Maintenance | Status | Tools | Wizard | Data Center | Help | Health
CMC Settings

Account Settings

Username: 192.168.64.65

Password:

Confirm:

WebAgent Settings

Primary WebAgent: 200.200.40.24:5000

Secondary WebAgent:

Shared Key:

Confirm:

CMC Location

Reside on the Same LAN? ● Yes ○ No

Total Bandwidth

Total Bandwidth of WAN Lines: Outbound: 100 Mbps Inbound: 100 Mbps

Traffic Alarm

Alarm is triggered when average outbound bandwidth usage over successive 30 minutes reaches 95 %

Alarm is triggered when average inbound bandwidth usage over successive 30 minutes reaches 85 %

3. Specify the following information.
   - **Username**

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

   - **Password, Confirm**

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

   - **Primary WebAgent, Secondary 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.

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.

- **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.

- **Shared Key, Confirm**

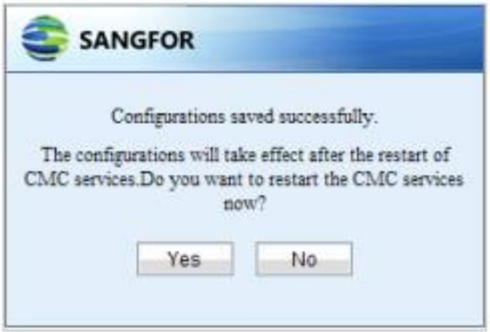
  Enter the shared key which should be the same as that configured on the CMC. Ignore it if no shared key is set on the CMC. This shared key is used for encrypting data transferred between the site and CMC.

- **Reside on the Same LAN?**

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

  The username, password and shared key should be identical with the site name, password and shared key configured on the CMC; otherwise, connecting to the CMC will fail.

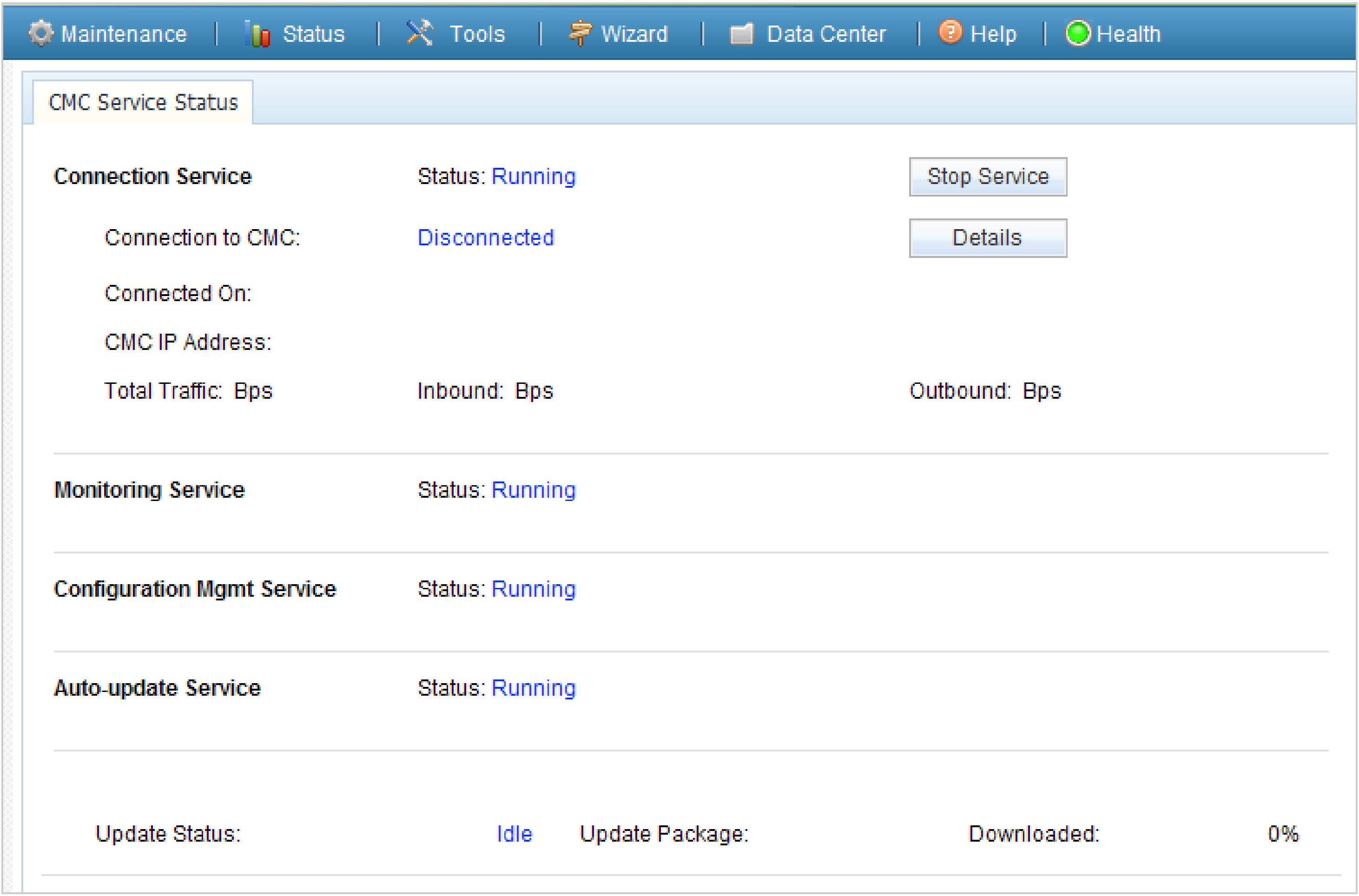
4. Click Save to save your settings, and the following prompt pops up:



Configurations saved successfully.

The configurations will take effect after the restart of CMC services.Do you want to restart the CMC services now?

5. Click yes to apply the settings or click No if you plan to restart them later.
6. To view whether the WOC is connected to the CMC, click Status > CMC Service Status on the toolbar at the top of the page to open the CMC Service Status page. As the Connection to CMC field shows, Connected means the WOC is connected to the CMC; otherwise, it means the connection is closed or not established.



Connection Service Status: Running

Connection to CMC: Disconnected

Connected On:

CMC IP Address:

Total Traffic: Bps Inbound: Bps Outbound: Bps

Monitoring Service Status: Running

Configuration Mgmt Service Status: Running

Auto-update Service Status: Running

Update Status: Idle Update Package: Downloaded: 0%

3.0 CMC Configuration

The purpose of having the distributed WOCs connect to the CMC is to conveniently manage, update and monitor them through the CMC.

In terms of privileges and administrative realms, administrators fall into the following three types: super administrator, group administrator and common administrator.

To learn more about the management by CMC, refer to the following:

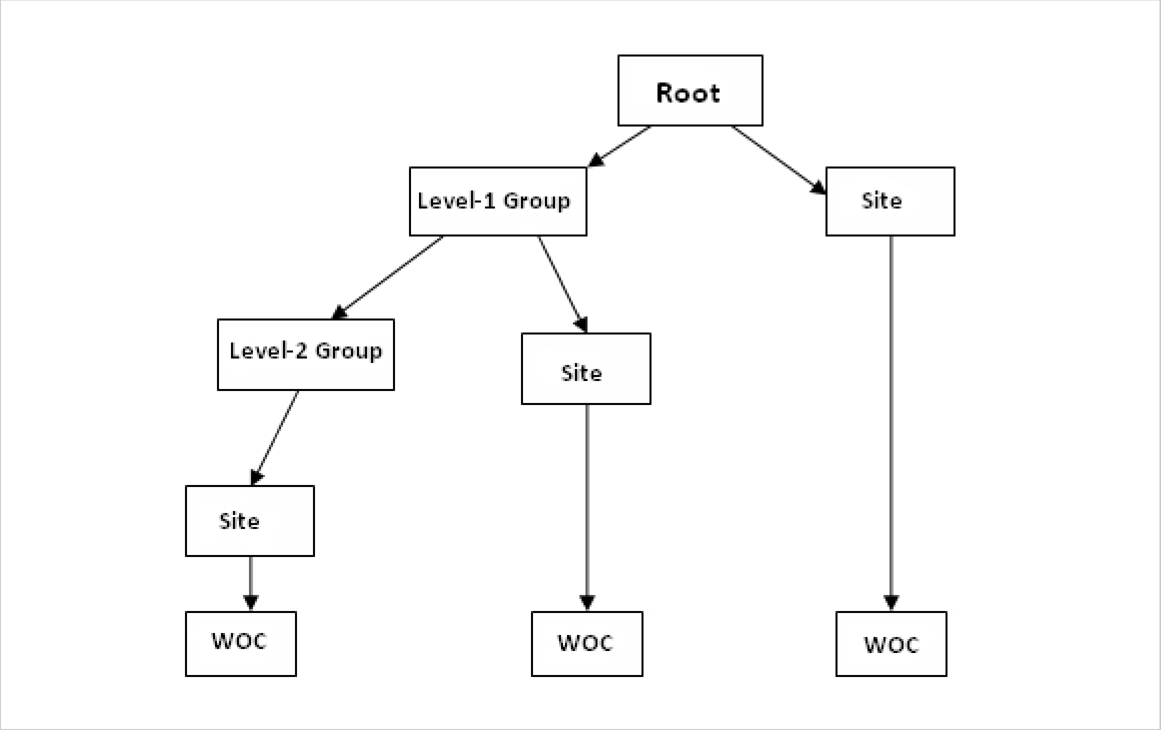
1. The hierarchical organization consisting of groups and sites (see Hierarchical Organization).
2. Administrator Privileges (see Administrators).

3.1 Hierarchical Organization

Overview

In most organizations, the privileges of staff are managed hierarchically and the higher-level divisions can give commands to the lower-level divisions.

The hierarchical management on the Sangfor Central Management Console (CMC) is just based on the same ideas. The CMC introduces the concepts of groups and sites and allows each level of group having its own subgroups and sites, which forms a tree-like structure. In this structure, settings on a group will be enforced on its subgroups and sites. This kind of configuration enforcement is similar to the above hierarchical privilege management in organizations.



Concept

Group: A group is a collection of subgroups and sites. The settings on a group will also apply to its subgroups and sites

Site: A site is a logical device created on the CMC. It is actually referred to as a remote physical WAN Optimization Controller (WOC) connecting to the CMC, and therefore you can manage remote physical WOCs through managing the sites created on the CMC.

WOC: A physical WAN Optimization Controller referred to as the site created on the CMC.

When optimization or bandwidth management (BM) is enabled/disabled for a group, they are also enabled/disabled for its subgroups and sites.

3.2 Administrators

Overview

Administrators of the Sangfor Central Management Console (CMC) configure and maintain the CMC as well as the distributed WAN Optimization Controllers (WOCs) that are connecting to the CMC. However, administrators of different roles have different privileges.

Administrator Roles

Super Administrator

By default, super administrators have the full privileges to view and edit all the groups and sites. Their privileges and administrative realms cannot be modified.

Group Administrator

By default, group administrators are granted the EDIT privilege, which cannot be modified. They can be assigned different realms so that they can only view and edit the groups/sites within their respective administrative realms.

Common Administrator

By default, common administrators are granted the VIEW privilege, which can be modified to be the EDIT privilege. Common administrators can also be assigned different administrative realms.

Privileges

The VIEW Privilege

If an administrator (common administrators typically) is assigned the VIEW privilege, it can only view the groups/sites within its administrative realm, which means the administrator cannot edit any groups/sites.

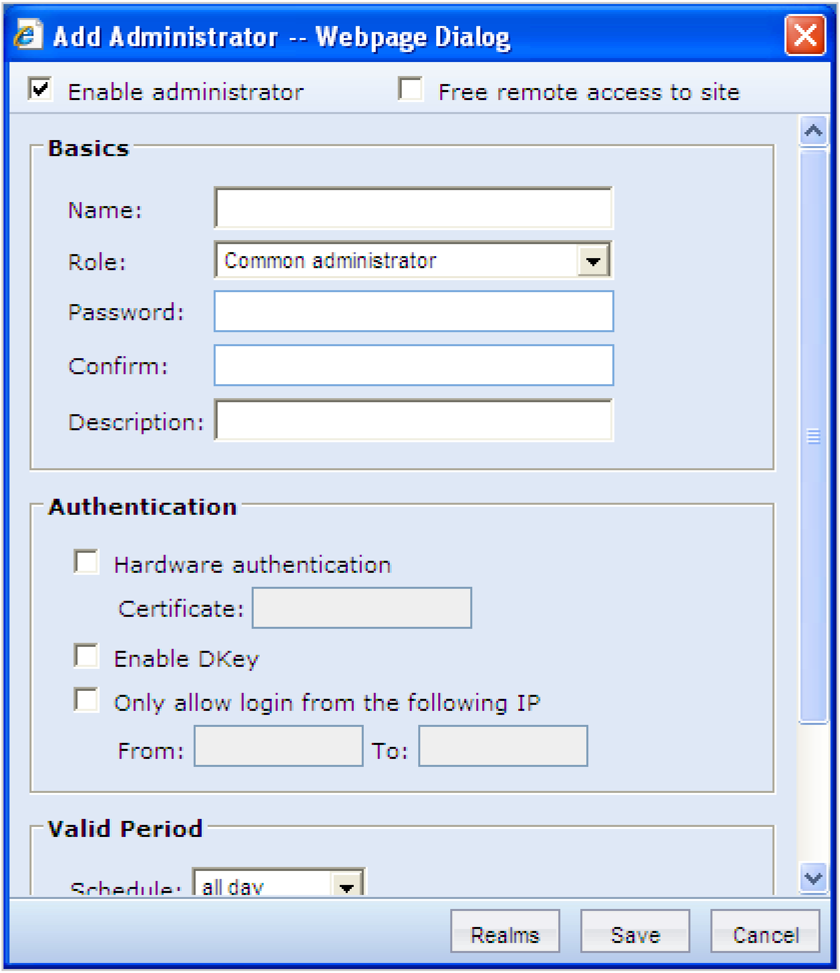
The EDIT Privilege

If an administrator is assigned the EDIT privilege, it can view and edit the groups/sites only within its administrative realm.

Creating an Administrator

To create an administrator,

1. Log into the administrator console of the CMC.
2. Go to the System > Administrators page, click Add to open the Add Administrator page and then specify the information for the administrator.



Add Administrator -- Webpage Dialog

☑ Enable administrator　□ Free remote access to site

Basics

Name:

Role: Common administrator

Password:

Confirm:

Description:

Authentication

□ Hardware authentication

Certificate:

□ Enable DKey

□ Only allow login from the following IP

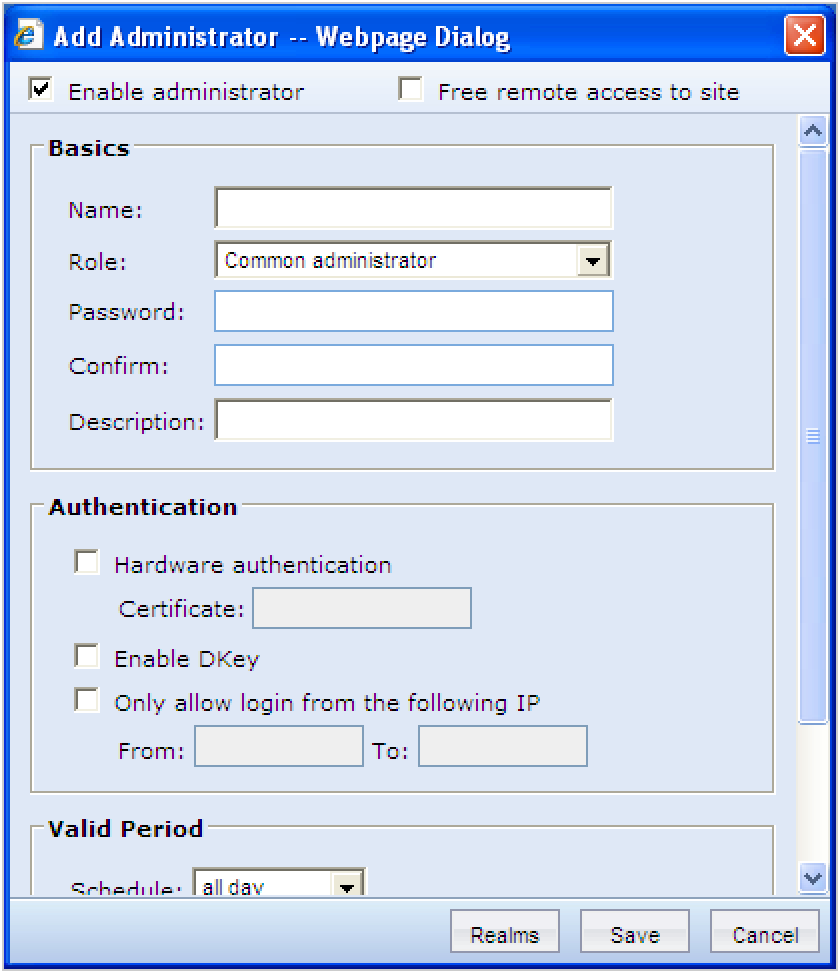
From: To:

Valid Period

Schedule: all day

Please pay attention to the role selection for different roles define different privileges. Administrators of lower-level role may fail to edit or configure certain groups/sites.

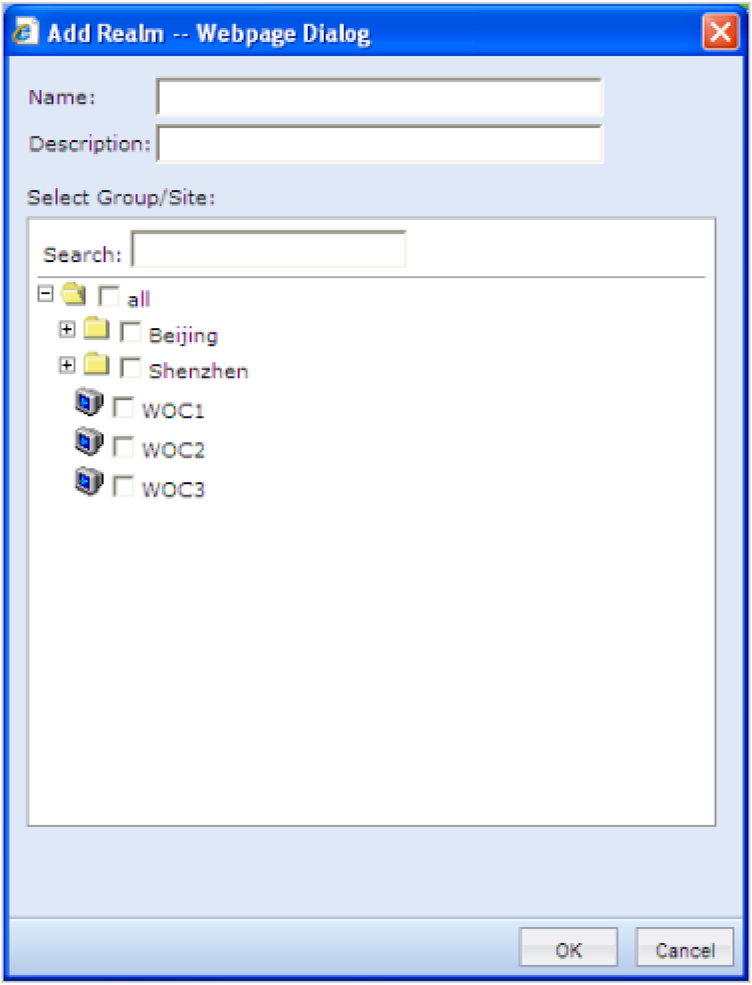
3. To view or configure the privilege for the administrator, click Realms to open the Administrative Realms page, which displays the default privilege for the administrator. Select the VIEW or EDIT privilege or only view the privilege configured for the administrator.



Add Administrator -- Webpage Dialog
☑ Enable administrator
□ Free remote access to site
Basics
Name:
Role: Common administrator
Password:
Confirm:
Description:
Authentication
□ Hardware authentication
Certificate:
□ Enable DKey
□ Only allow login from the following IP
From:
To:
Valid Period
Schedule: all day
Realms
Save
Cancel

The Realms button is available for group and common administrators only. However, you can only configure the administrative realms for group administrator, while for the common administrators, you can configure the realms as well as the privilege. For super administrators, both the realms and privilege are not allowed to be modified and therefore the Realms button is disabled.

4. Click Add to open the Add Realm page, which displays all the available groups and sites. Select the groups and sites that the administrator can administer (edit or view only).



5. Click OK and then Save to apply the settings.

4.0 Information Monitoring

Contents

After sites connect to the Central Management Console (CMC), CMC administrators can conveniently check the network status, optimization status or other information of the sites through the CMC administrator console. The CMC provides the real-time information of sites through the following ways:

- Emails anomalous events to the specified email address once they occur on the sites (see Email Alarm).
- Displays real-time information of sites (see Site Summary).
- Supports remote login to sites to view the information (see Remote Control).
- Shows the optimization status of the sites (see Optimization Status).

4.1 Email Alarm

Overview

When an alarm-triggering event occurs on any site (WOC), the CMC will generate and email an alert message to the specified email address. Each administrator can select the alarm-triggering events and specify the recipient email address of his or her own. These settings configured by an administrator are independent and invisible to any other administrators, and therefore administrators can only receive the alert messages related to the sites within their respective realms.

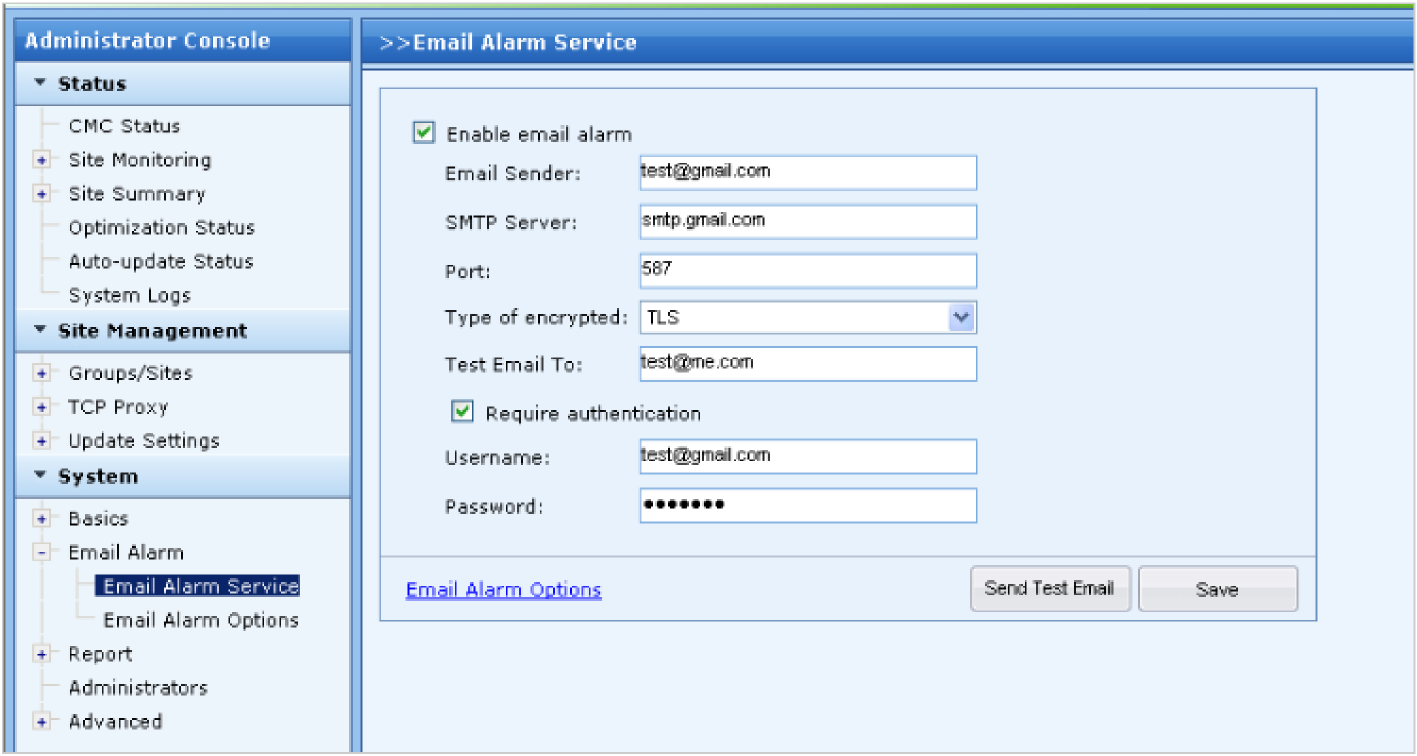
To have the Email Alarm function work, do the following:

1. Enable the Email Alarm function and specify the SMTP server (on the Email Alarm Service page).
2. Select alarm-triggering events and specify an email address to receive the email notifying the events (on the Email Alarm Options page).

Email Alarm Service

You can enable the Email Alarm function and specify the SMTP server on this page.

1. Go to the System > Email Alarm Service page, as shown below:



☑ Enable email alarm

Email Sender: test@gmail.com

SMTP Server: smtp.gmail.com

Port: 587

Type of encrypted: TLS

Test Email To: test@me.com

☑ Require authentication

Username: test@gmail.com

Password: •••••••

2. Specify the following information.
   - **Enable email alarm**

     Check it to enable the email alarm function; otherwise, no email will be sent even the email alarm is triggered by anomalous events.

   - **Email Sender**

     Specify the email address from which the alert messages will be emailed.

   - **SMTP Server**

     Enter the address of the SMTP server for sending emails. After that, click Send Test Email to test if the SMTP server is available.

   - **Test Email To**

     Enter the email address to which the email will be sent for testing the connectivity of the SMTP sever.

   - **Require authentication**

Check the option and type username and password if authentication is expected on login to the SMTP server.

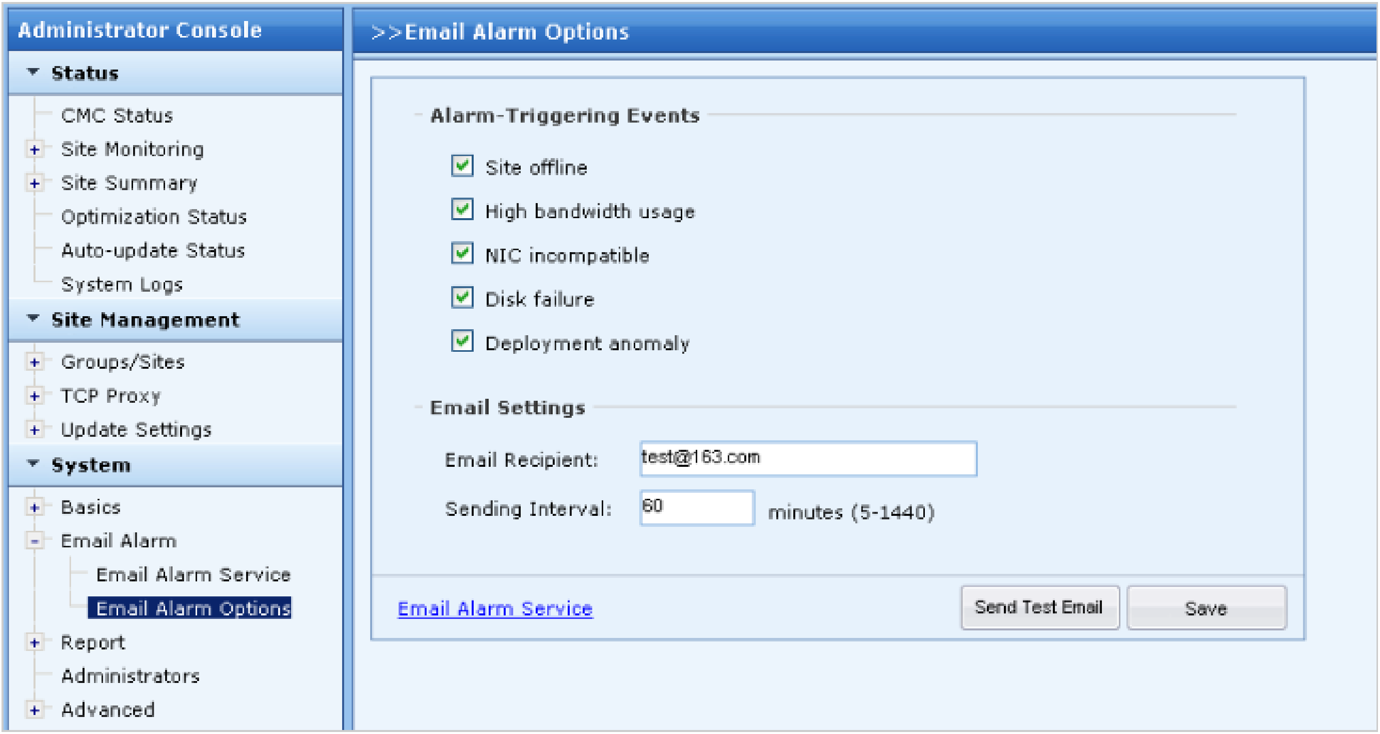
The above options are available only to super administrators and are read-only for other administrators.

3. Click Save to apply the settings.

Email Alarm Options

You can select the alarm-triggering events and specify an email address to receive the corresponding alert messages on this page.

1. Go to the System > Email Alarm Options page, as shown below:



Alarm-Triggering Events

☑ Site offline

☑ High bandwidth usage

☑ NIC incompatible

☑ Disk failure

☑ Deployment anomaly

Email Settings

Email Recipient: test@163.com

Sending Interval: 60 minutes (5-1440)

2. To have an anomalous event monitored, check the event (for more information about the alarm-triggering events, see the subsequent section).
3. Specify the email address of the recipient and sending frequency.

   When an alarm-triggering event occurs on a site (WOC), an alert message will generated and emailed to the email address specified here and the administrators whose administrative realm covers the site. If an administrator is deleted, no email will be sent to the email address specified by that administrator.

Sending Interval ranges from 5 to 1440 minutes. By default, it is 720 minutes, which means alert messages will be emailed every 720 minutes. For the events occurred within the specified interval, the corresponding emails will be generated and collected. After the interval, the emails for the same type of events will be combined into one email and then sent to the administrator. For this reason, the time when the email is generated may differ from the time when the email is sent. Email body is limited to 8K bytes. If email body is larger than 8K bytes, only the first 8K content will be sent, with the rest dropped.

4. Click Save to apply the settings.

Alarm-triggering Events

Currently, the CMC generates and emails alert messages for the following events:

- **Site offline**

  Once a site gets offline, the CMC generates an alert message immediately. When the site then gets online, the CMC also generates an alert message. These alert messages will be emailed to the corresponding administrator(s) if the site has been offline for more than 30 minutes.

- **Site enables bypass**

  When a site enables bypass, the CMC generates an alert message immediately. When the site then disables bypass, the CMC also generates an alert message. These alert messages will be emailed to the corresponding administrator(s) if bypass has been enabled for more than 30 minutes.

- **High bandwidth usage**

  Every time any of the bandwidth usage thresholds configured on a site is exceeded, the CMC generates and emails an alert message.

- **NIC incompatible**

  When there is a high packet loss rate or a large number of error packets on any NIC of a site, the CMC generates an alert message. The alert message will be emailed to the corresponding administrator(s) if this kind of anomalous event lasts for more than 10 minutes.

- **Disk failure**

  Disk health status is checked by the smartctl utility. Once the disk of a site (WOC) is detected unhealthy, the CMC generates and emails an alert message.

- **Deployment anomaly**

Once cables are detected inversely connected or unplugged on a site (WOC) deployed under Bridge or Double-bridge mode, the CMC generates an alert message. The alert message will be emailed to the corresponding administrator(s) if this kind of anomalous event lasts for more than 10 minutes.

The alert messages for the above events to be emailed are as follows:

1. Site offline:

   Subject: Alarm - Site Was Offline

   Content: The site xxx has been offline since 2010-8-28 12:04:00. Please contact the site administrator timely.

2. Site enables bypass:

   Subject: Alarm - Site Enabled Bypass

   Content: The site xxx has enabled bypass since 2010-8-28 12:04:00. Please contact the site administrator timely.

3. High bandwidth usage:

   Subject: Alarm - High Bandwidth Usage

   Content: The average outbound bandwidth usage of the site XXX during 2012-8-28 12:04:00 - 2012-8-28 13:04:00 reached 95%, which exceeds the threshold 70%. Please contact the site administrator timely.

4. NIC incompatible

   Subject: Alarm - NIC Incompatible

   Content: NIC incompatibility was detected on the site XXX at 2012-8-28 12:04:00. Please contact the site administrator timely. Details:

NIC	rx_packets	rx_errors	rx_overruns	tx_packets	tx_errors	tx_overruns	collisions
eth0	45729658	6568996	6651	34427	28996	997	0
eth1	45677105	0	0	207	0	0	0
eth2	1819850	0	0	244024	0	0	0

5. Disk failure:

   Subject: Alarm - Disk Failure

   Content: Disk failure was detected on the site XXX at 2012-8-28 12:04:00. Please contact the site administrator timely. Details:

   ```
   smartctl version 5.38 [i686-pc-linux-gnu] Copyright (C) 2002-8 Bruce Allen
   Home page is http://smartmontools.sourceforge.net/

   SMART support is: Unavailable - device lacks SMART capability.
   Checking to be sure by trying SMART ENABLE command.
   Error SMART Enable failed: Input/output error
   SMART ENABLE failed - this establishes that this device lacks SMART functionality.
   A mandatory SMART command failed: exiting. To continue, add one or more '-T permissive' options.
   ```

6. Deployment anomaly:

   Subject: Alarm - Deployment Anomaly

   Content: Deployment anomaly was detected on the site XXX at 2012-8-28 12:04:00. Please contact the site administrator timely. Details:

   ```
   WAN1(eth2): no link;
   The cables connecting br0 LAN and WAN1 interfaces are inversely used. Please use the cables correctly.
   The cables connecting br1 DMZ and WAN2 interfaces are inversely used. Please use the cables correctly.
   ```

Scenario

1. Alarm on site offline
   - Assume: The email alarm function is not enabled.

     Results: The options on the Email Alarm Options are not configurable.

   - Assume: The email alarm function is enabled, but SMTP server and test email recipient are not specified.

     Results: The page is configurable. Check the alarm-triggering event and click Save. The prompt will pop up saying: the recipient email address is required.

   - Assume: The email alarm function is enabled and related parameters are correctly configured. Both Admin01 and Admin check the "site offline" event to be monitored, and Admin01 specifies its recipient address while Admin02 not. The site S1 is in the administrative realms of both Admin01 and Admin02. Now, S1 gets offline.

Results: Admin01 will receive the email while Admin02 will not. If the site is not in Admin01's administrative realm, Admin01 will not receive the email either.

- Assume: The site was offline due to network interruption and then back to normal after 5 minutes

  Results: The CMC logs the event without emailing it to the administrator.

- Assume: The site has been offline for more than 30 minutes

  Results: The CMC logs the event and email it to the administrator after 30 minutes.

2. Alarm on site bypass
   - Assume: The email alarm function is enabled and related parameters are correctly configured. A site named S1 has connected to the CMC and Admin01 checks the "site enabled bypass" event to be monitored and specifies an email address to receive the alert email. Now, S1 enables bypass.

     Results: The site reports the event to the CMC, which will then email the event to Amdin01.

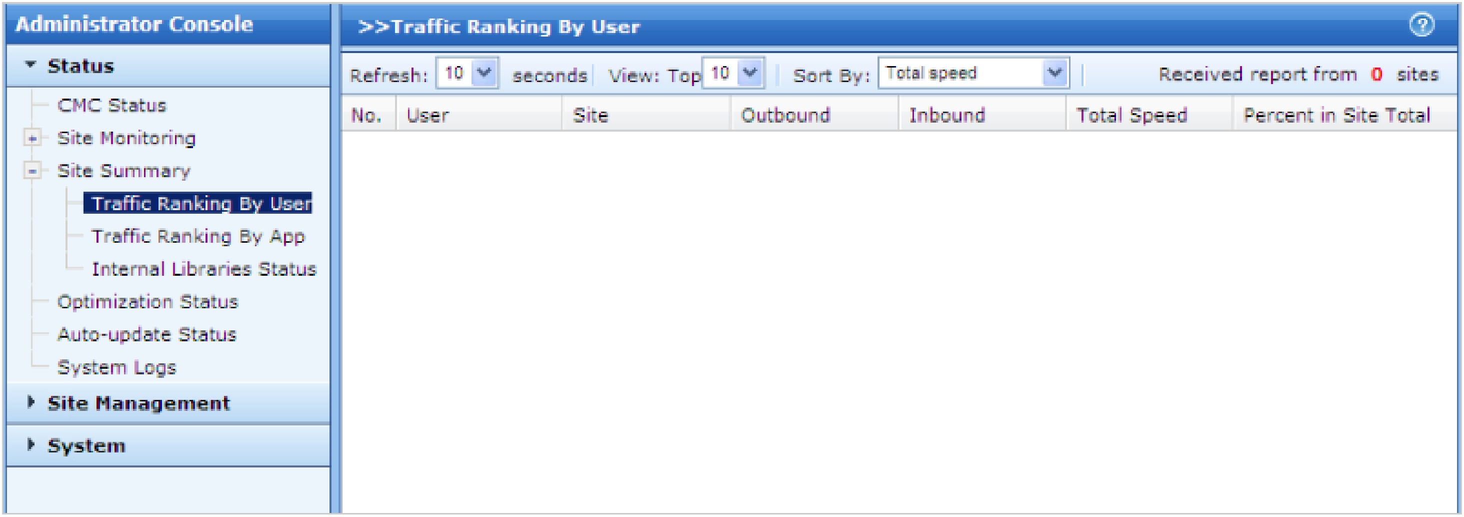
4.2 Site Summary

Overview

Site Summary displays the real-time information about all sites, including traffic ranking by user, traffic ranking by application and internal libraries status. The statistics provide underlying insight needed for CMC administrators to diagnose problems and manage WAN Optimization Controllers (WOCs) distributed across a WAN.

Traffic Ranking By User

The Traffic Ranking By User page displays the top 10, 20 or 30 users out of all site users that cause the most traffic per unit time. Go to the Status > Site Summary > Traffic Ranking By User page, as shown below:



Refresh: 10 seconds | View: Top 10 | Sort By: Total speed | Received report from 0 sites

No.	User	Site	Outbound	Inbound	Total Speed	Percent in Site Total

- **Refresh**

  Specify the refresh interval to have the information automatically refreshed. Options are 5, 10, 20 or 60 seconds. By default, it is 10 seconds.

- **View Top**

  Select 10, 20 or 30 to specify the number of users top ranked in terms of traffic caused per unit time. By default, only the top 10 users are displayed.

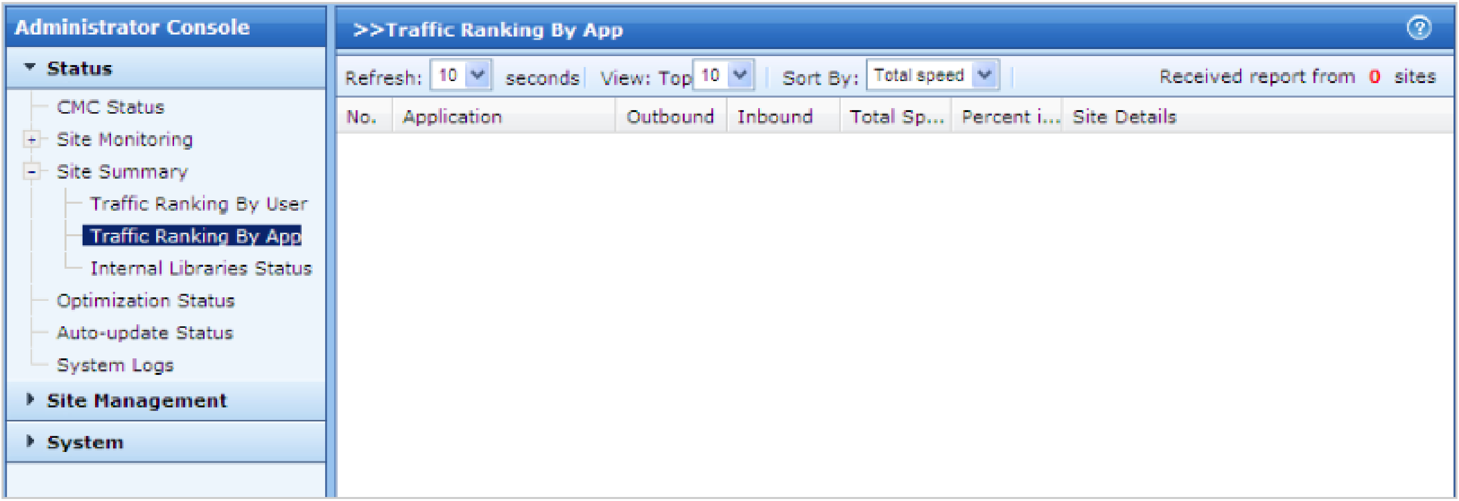
- **Sort By**

  Select an item based on which the entries are sorted in descending order. Options are outbound speed, inbound speed, total speed and percent in site total.

The unit of speed is b/s; however, the unit Kb/s, Mb/s or Gb/s may also be used when the speed is high.

Traffic Ranking By Application

The Traffic Ranking By App page displays the top 10, 20 or 30 applications out of all site applications that cause the most traffic per unit time. Go to the Status > Site Summary > Traffic Ranking By App page, as shown below:



Refresh: 10 seconds | View: Top 10 | Sort By: Total speed | Received report from 0 sites

No.	Application	Outbound	Inbound	Total Sp...	Percent i...	Site Details

- **Refresh**

  Specify the refresh interval to have the information automatically refreshed. Options are 5, 10, 20 or 60 seconds. By default, it is 10 seconds.

- **View Top**

  Select 10, 20 or 30 to specify the number of applications top ranked in terms of traffic caused per unit time. By default, only the top 10 applications are displayed.

- **Sort By**

  Select an item based on which the entries are sorted in descending order. Options are outbound speed, inbound speed and total speed.

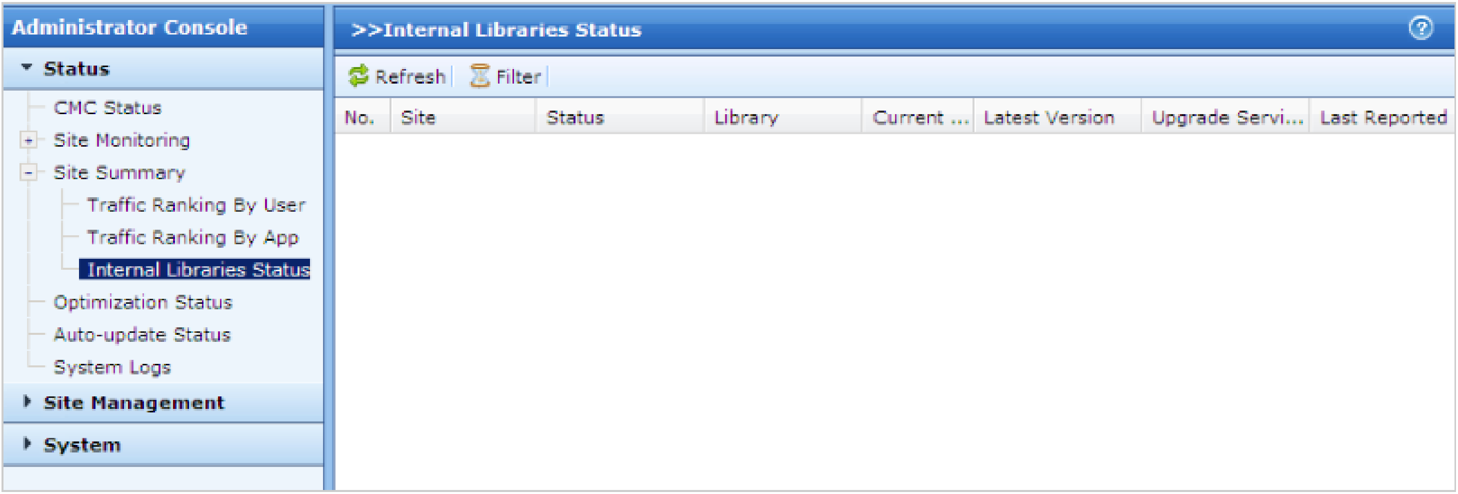
- **Site Details**

  View the corresponding sites (up to 3 sites). You can click the TCP Proxy link to set the TCP proxy rule for the site.

The unit of speed is b/s; however, the unit Kb/s, Mb/s or Gb/s may also be used when the speed is high.

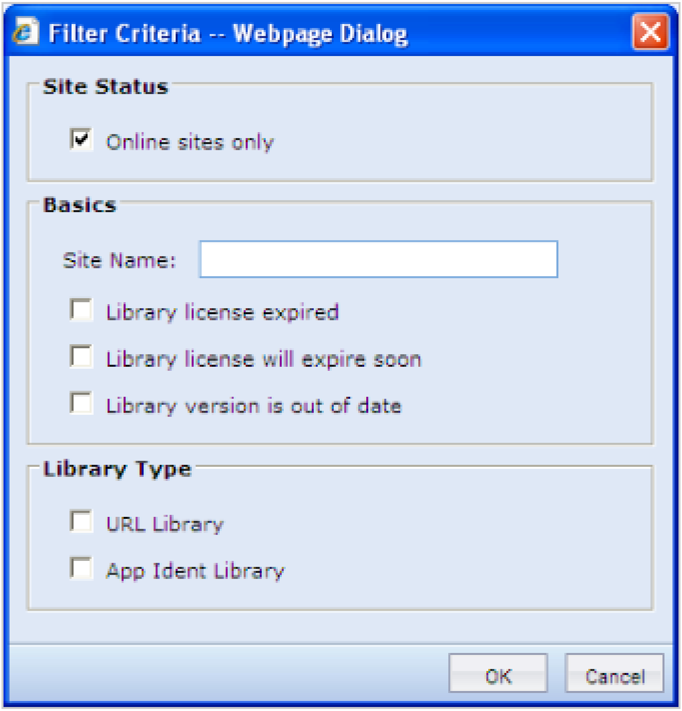
Internal Libraries Status

The Internal Libraries Status displays the status of the built-in libraries of all or online sites. Go to the Status > Site Summary > Internal Libraries Status page, as shown below:



Click Refresh to have all the online sites report the status of their internal libraries. Please note that the interval between two adjacent refresh operations should be no less than 60 seconds. The library status information displayed on this page are reported by the sites and will be preserved until the sites report new status information. Last Reported indicates the last time when the information is reported.

To view the information of specific sites, click Filter to open the Filter Criteria dialog, as shown below:



Filter Criteria -- Webpage Dialog

Site Status

☑ Online sites only

Basics

Site Name:

☐ Library license expired

☐ Library license will expire soon

☐ Library version is out of date

Library Type

☐ URL Library

☐ App Ident Library

- **Site Status**

  Specify whether to view the internal libraries status of online sites only.

- **Basics**

  Enter a keyword of the site name to start a fuzzy search (if none is typed, all site names will be matched) and specify other options to filter the display.

- **Library Type**

  Check URL library or/and APP Ident Library so that only the status information of the specified libraries will be displayed. Status information about libraries includes Current Version, Latest Version and Upgrade Service Expires, which is reported by the corresponding sites earlier every morning.

  Anomalous events will be highlighted in different colors:
  The messages "Library license expired" and "Library version is out of date" will be highlighted in red, and the message "Library license will expire soon" will be highlighted in blue.

4.3 Remote Control

Overview

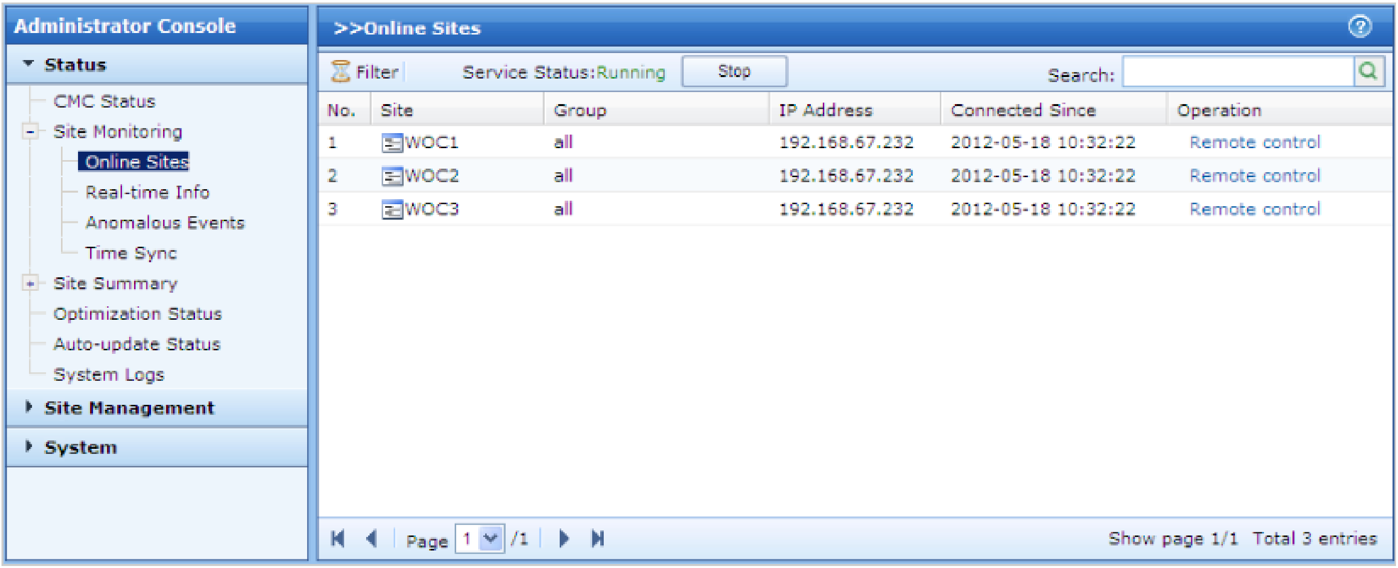
The Central Management Console (CMC) provides the remote control function, which enables CMC administrators to remotely access the administrator console or Data Center of sites within their administrative realms to configure sites or view logs.

Remote Access to a Site

When an administrator is remotely logging into a site, the authentication may be or may not be required. It depends on whether the **Free remote access to site** option (see the subsequent section) is checked for the administrator. If the option is checked for the administrator, he or she can directly log into the administrator console or Data Center of the site as **admin** (super admin of the site) without entering any credentials; otherwise, the administrator needs to enter the username and password of an administrator account of the site to login.

To remotely log into the administrator console or Data Center of a site,

1. Go to the Status > Site Monitoring > Online Sites page to view the online sites, as shown below:

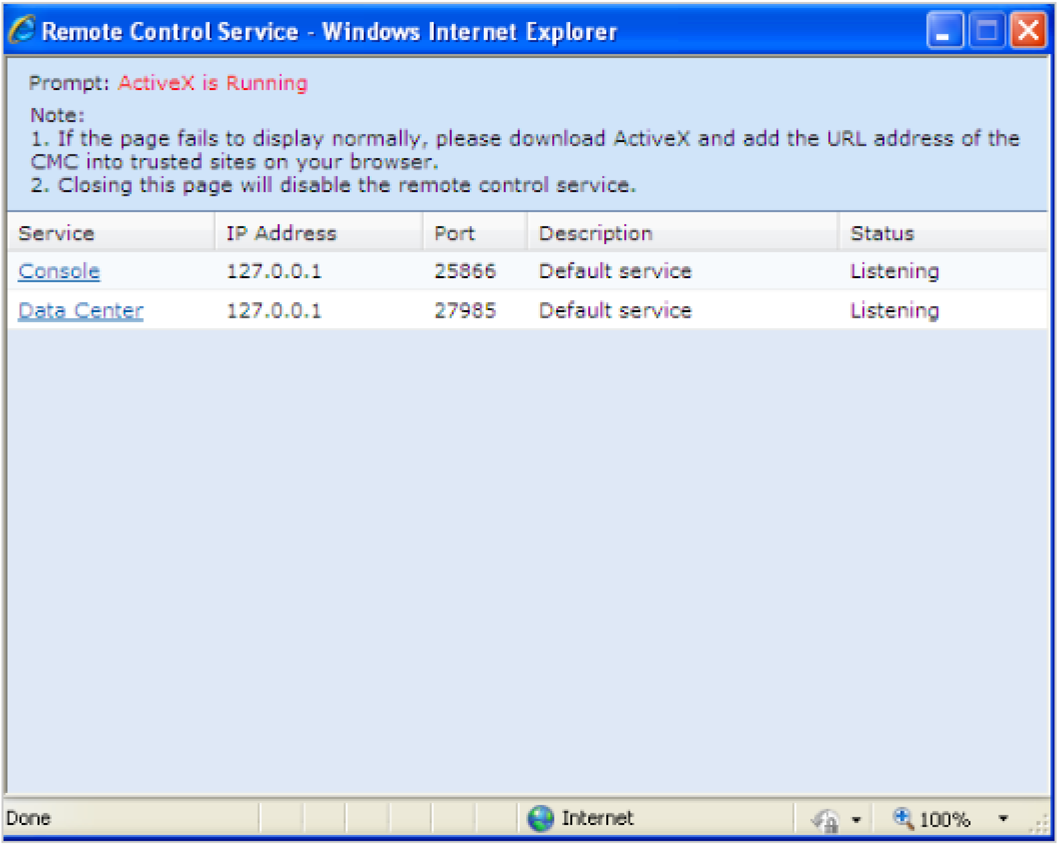


Service Status:Running

No.	Site	Group	IP Address	Connected Since	Operation
1	WOC1	all	192.168.67.232	2012-05-18 10:32:22	Remote control
2	WOC2	all	192.168.67.232	2012-05-18 10:32:22	Remote control
3	WOC3	all	192.168.67.232	2012-05-18 10:32:22	Remote control

Show page 1/1 Total 3 entries

2. Click the Remote Control link to open the Remote Control Service page, as shown below:



Prompt: ActiveX is Running

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 disable the remote control service.

Service	IP Address	Port	Description	Status
Console	127.0.0.1	25866	Default service	Listening
Data Center	127.0.0.1	27985	Default service	Listening

3. Click the Console or Data Center link to remotely access the administrator console or Data Center of the site.

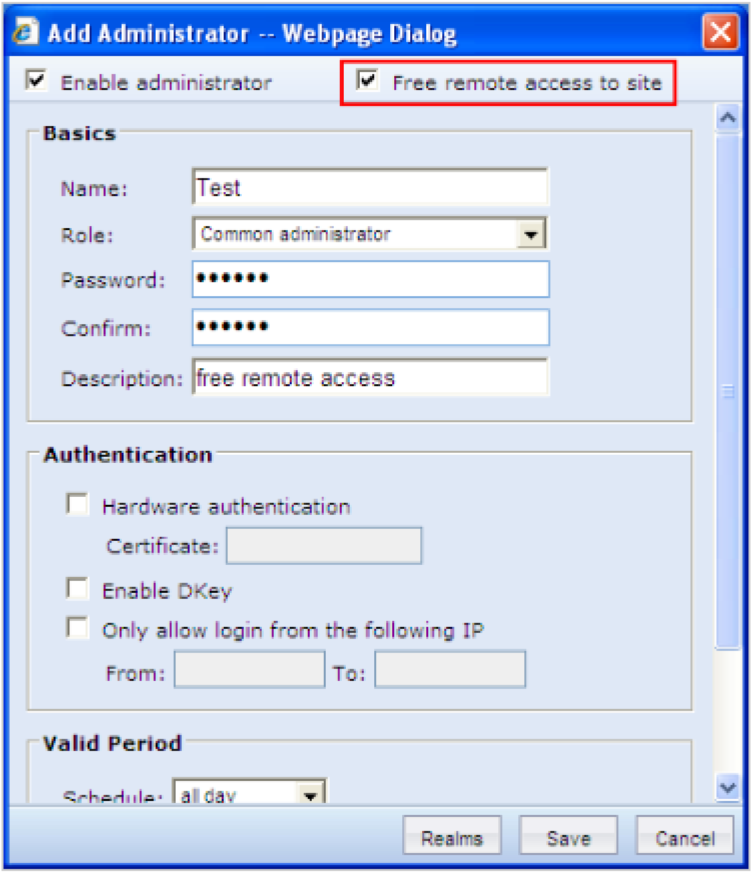
Do NOT close the Remote Control Service page during remote access to the site; otherwise, the remote access session will be disconnected.
All the operations and configurations performed on the site (WOC) by the CMC administrator will be logged, just as they are performed by the corresponding site administrator.

Free Remote Access to Site

Administrators with the **Free remote access to site** privilege can directly login to the administrator console or Data Center of a site as **admin** (super admin of the site) simply by clicking the Console or Data Center link. Without such a privilege, administrators need to enter the username and password of an administrator account of the site.

To add an administrator that can remotely login to a site without entering any credentials, go to the System > Administrators page, click Add to open the Add Administrator page, check the **Free remote access to site** option and specify other information, as shown below:

The **Free remote access to site** option is available only when you are logged into the CMC as a super administrator.



Add Administrator -- Webpage Dialog

☑ Enable administrator ☑ Free remote access to site

Basics

Name: Test

Role: Common administrator

Password: ••••••

Confirm: ••••••

Description: free remote access

Authentication

□ Hardware authentication

Certificate:

□ Enable DKey

□ Only allow login from the following IP

From: To:

Valid Period

Schedule: all day

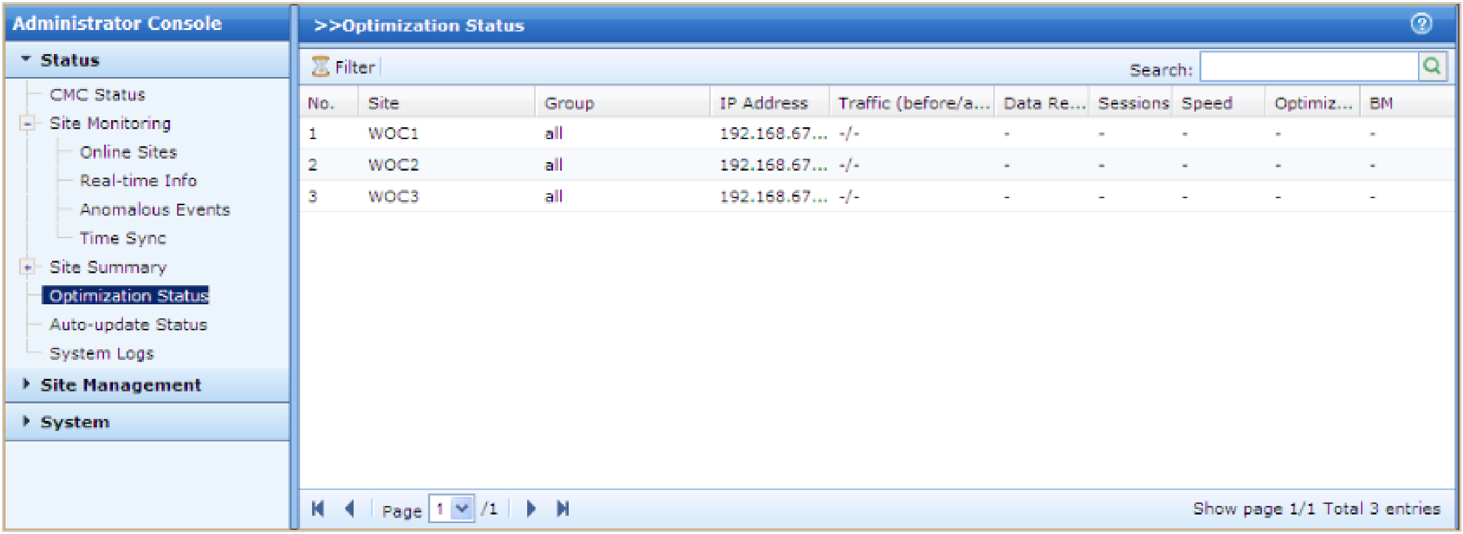
4.4 Optimization Status

Overview

This Optimization Status page mainly displays the optimization-related information about the Sangfor WAN Optimization Controllers (WOCs) connecting to the CMC.

Optimization Status

The Optimization Status page displays the optimization information about each connecting WOC, including traffic before/after optimization, data reduction rate, number of sessions, speed, optimization status and bandwidth management status, as shown in the following figure:



No.	Site	Group	IP Address	Traffic (before/a...	Data Re...	Sessions	Speed	Optimiz...	BM
1	WOC1	all	192.168.67...	-/-	-	-	-	-	-
2	WOC2	all	192.168.67...	-/-	-	-	-	-	-
3	WOC3	all	192.168.67...	-/-	-	-	-	-	-