

## Cloud Network Center/Cloud Network Agent

CNC

CNA100

Cloud Center

Firmware Version 1.4.0  
Edition 3, 6/2017

## Application Note

Default Login Details	
Service Port IP Address	https://169.254.1.3
User Name	admin
Password	1234

This handbook is a series of tutorials that guides you through various applications of the Zyxel Cloud Network Center. The purpose of the handbook is to show you how to proceed through an application rather than explain the meaning of GUI features.

Note: IP addresses, port numbers, and object names are just examples used in these tutorials, so you must replace them with the corresponding information from your own network environment when implementing a tutorial.

Bold text indicates the name of a GUI menu, field or field choice.

The handbook is for a series of products. Not all products support all firmware features. Screenshots and graphics in this handbook may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this handbook is accurate at the time of writing.



## Topic

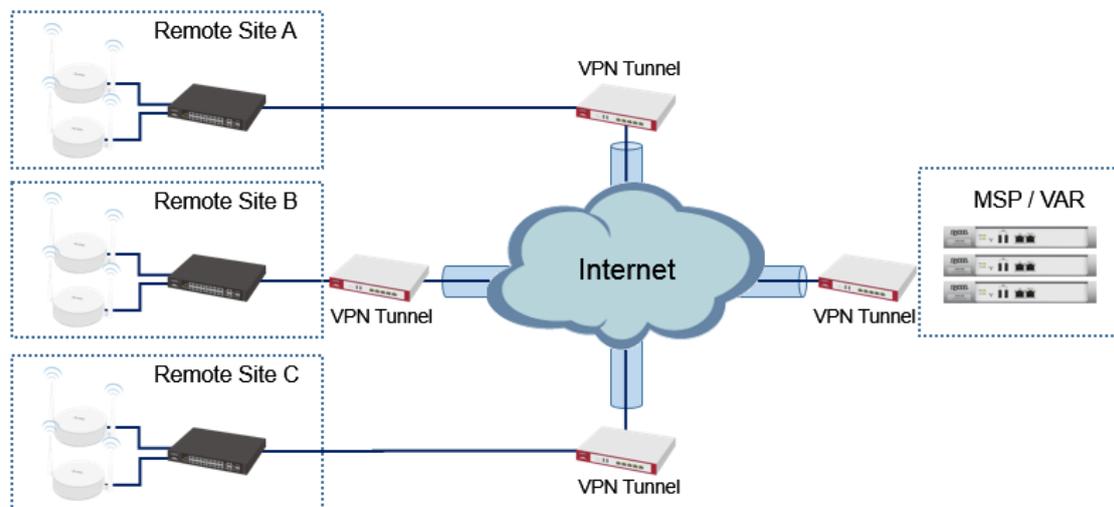
1	How to Deploy and Install the Cloud Network Agent .....	5
1.1	Initial Configurations.....	6
1.2	Verify that the CNA is Online .....	9
1.3	What Could Go Wrong? .....	9
2	How to Share or Transfer CNA Account Management .....	10
2.1	Managing Organization Operators .....	11
2.2	Verify that Accounts are Granted Privilege .....	12
2.3	What Could Go Wrong? .....	13
3	How to Provide Value Added Service using CNC .....	14
3.1	Discover Zyxel Devices in the Local Network.....	15
3.2	Schedule Firmware Upgrade.....	16
3.3	Interpreting Graphs and Node Performance .....	19
3.4	Receiving Email Notifications and Alerts during Link Failures .....	21
3.5	Backing-Up and Restoring Device Configurations.....	22
3.6	What Could Go Wrong? .....	25
4	How to Replace and Recover Failed Devices .....	27
4.1	Replacing Devices through Centralized Management.....	28
4.2	Replacing Devices through Remote Site Management.....	29
4.3	What Could Go Wrong? .....	33
5	How to Auto-Provision Zyxel Devices Using CNC Push CLI.....	35
5.1	Configuring the Administrator Password for Switches .....	36
5.2	Creating and Configuring VLAN for Switches.....	39
5.3	Scheduled PoE Port State for Switches .....	42
5.4	Configuring the Administrator Password for Access Points.....	45
5.5	Creating an SSID for Access Points .....	48
5.6	Creating Scheduled SSID for Access Points .....	51
5.8	Creating a VLAN for Security Gateways .....	57

5.9	Editing a VLAN IP Interface for Security Gateways .....	60
5.10	Verify that Push CLI is Successful .....	63
5.11	What Could Go Wrong? .....	65
6	How to Manage New Firmware Releases .....	66
6.1	Receiving New Firmware Notifications.....	66
6.2	Managing New Firmware Releases .....	68
7	How to Improve CNC Data Integrity .....	69
7.1	Enhancing Security through SNMPv3 .....	69
7.2	Verifying SNMPv3 Configurations .....	71
7.3	What May Go Wrong? .....	71

## 1 How to Deploy and Install the Cloud Network Agent

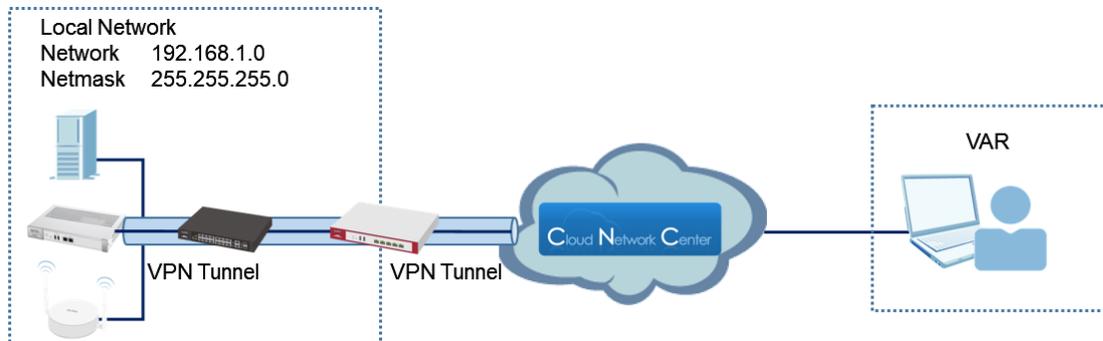
This example shows a **centralized management architecture**. In this architecture, service providers have already established VPN access to their client remote sites. **Cloud Network Agents (CNA)** are installed on the **Managed Services Provider's (MSP)** offices. **Value Added Resellers (VAR)** can monitor and maintain site devices anywhere with Internet access.

**Figure 1 Centralized Management through CNC**



This example shows a **remote site architecture**. In this architecture, the CNAs are installed in customer site. The CNA establishes VPN tunnel to CNC as soon as it receives Internet access. VARs can monitor and maintain site devices anywhere with Internet access.

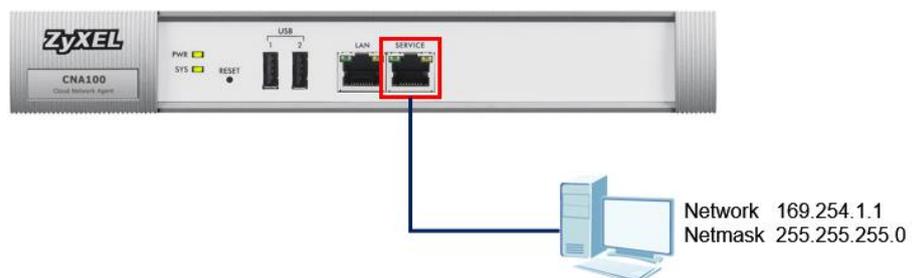
**Figure 2 Remote Site Management through CNC**



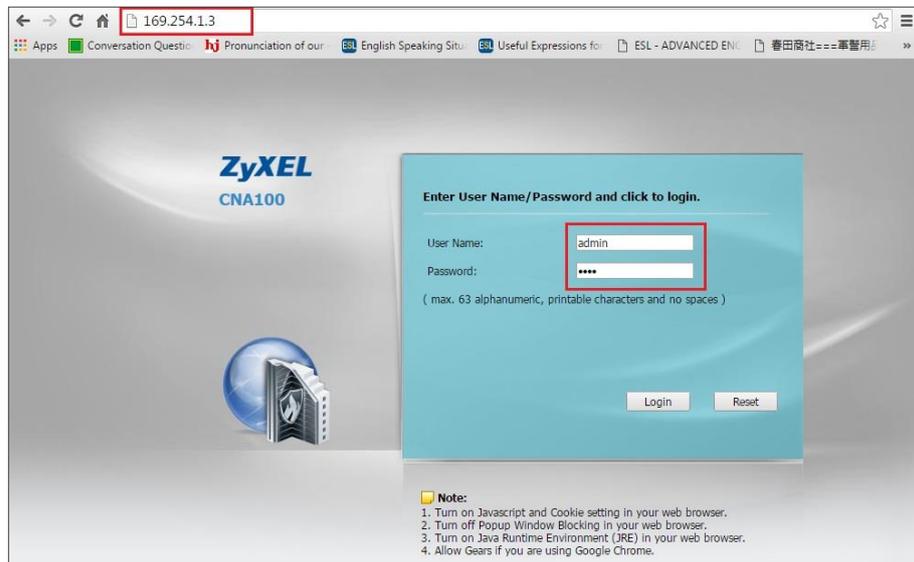
 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110, GS1920-24HP, NWA5123-NI, and CNA100.

## 1.1 Initial Configurations

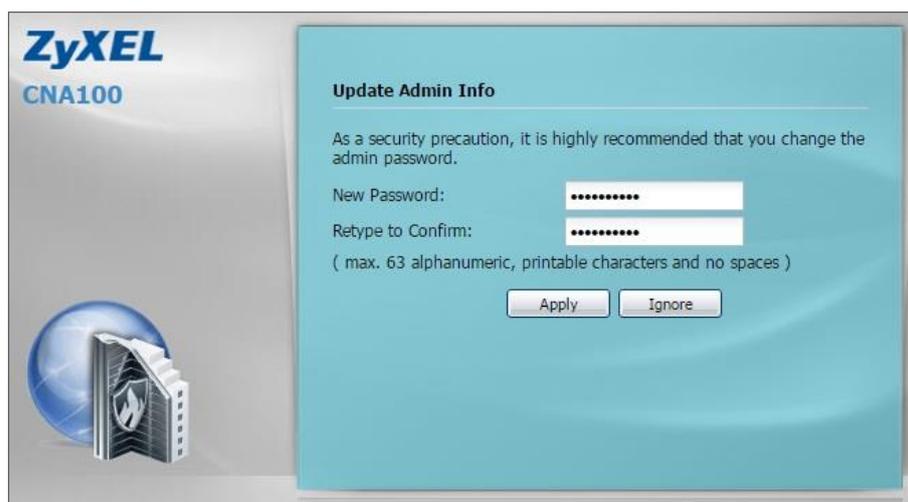
- 1 Configure PC IP Address to "169.254.1.1" and connect Ethernet cable to CNA's service port.



- 2 Access the CNA's Web GUI using IP address "169.254.1.3". Use the default administrator password.



- 3 For security purposes, it is strongly recommended to change the default admin password.



- 4 If you need to configure the CNA to use static IP addresses instead, go to **CONFIGURATION > Network > Interface** and edit LAN interface.

## CONFIGURATION > Network > Interface > LAN

**Edit Ethernet**

**Interface Properties**

Interface Name: LAN  
 Port: P1  
 MAC Address: A0:E4:CB:84:86:F8

**IP Address Assignment**

Get Automatically  
 Use Fixed IP Address

IP Address: 192.168.1.100  
 Subnet Mask: 255.255.255.0  
 Gateway: 192.168.1.1  
 First DNS Server: 8.8.8.8  
 Second DNS Server:

OK Cancel

- 5 For all **Zyxel Enterprise Switches**, access the CLI using Telnet/SSH/Console and configure “*display users*” and “*display aaa*”.

```
Switch# conf
Switch(config)# display user
Switch(config)# display aaa
```

- 💡 Note: The Zyxel Enterprise Switch models do not save the user password or aaa shared keys by default.
- 💡 Note: Failing to configure “display user” causes CNC's regular **Backup** and **Push CLI** to fail should the switch undergo reboot.

## 1.2 Verify that the CNA is Online

- 1 Log in to the Zyxel CNC with CNA ownership account, go to **Organization View**. CNA should appear as **online**.

### Organization View

Site	Devices	Tags	CNA	Action
Site X	3 0 0		Demo_2	

## 1.3 What Could Go Wrong?

- 1 If CNC does not display the CNA, CNA may be receiving an incorrect DHCP configuration. Use the ZON utility through the local network to verify the DHCP configurations. IP address configurations should be able to provide CNA access to the Internet.

### ZON > IP Configuration

IP Configuration

**ZyXEL**

IP Configuration

IPv4 setting : DHCP

IP address : 192 . 168 . 1 . 34

Subnet mask : 255 . 255 . 255 . 0

Gateway : 192 . 168 . 1 . 1

DNS1 : 192 . 168 . 1 . 1

DNS2 : 0 . 0 . 0 . 0

Info

System : cna100

Location :

Device administrator password

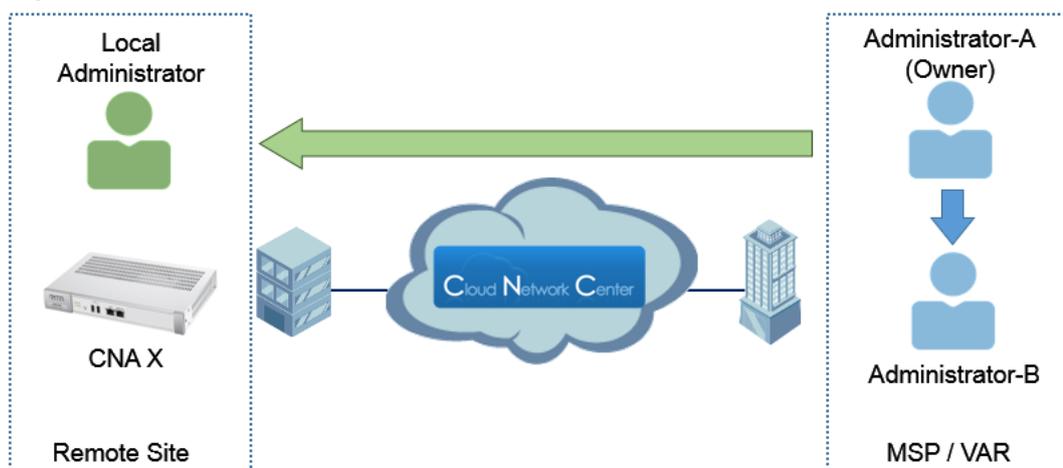
- 2 If the CNA needs to be configured with a static IP address but forgot the administrator password, press and hold down the "RESET" button on the CNA's front panel for 10 seconds. The administrator password revert to default after boot up.



## 2 How to Share or Transfer CNA Account Management

This example shows how to provide users authority to manage and monitor sites. This example will instruct CNA owners when to provide "read-only" or "full" privilege to different accounts.

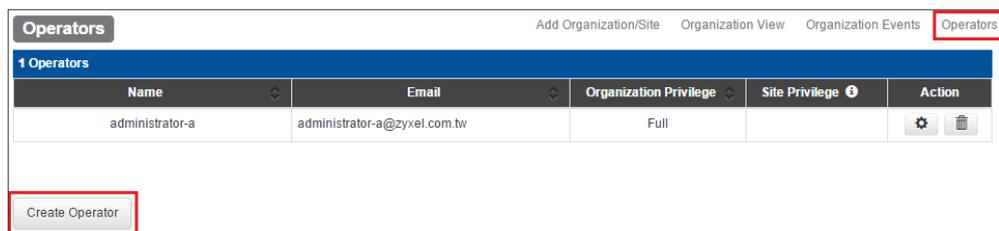
**Figure 3** Types of Site Administrators



## 2.1 Managing Organization Operators

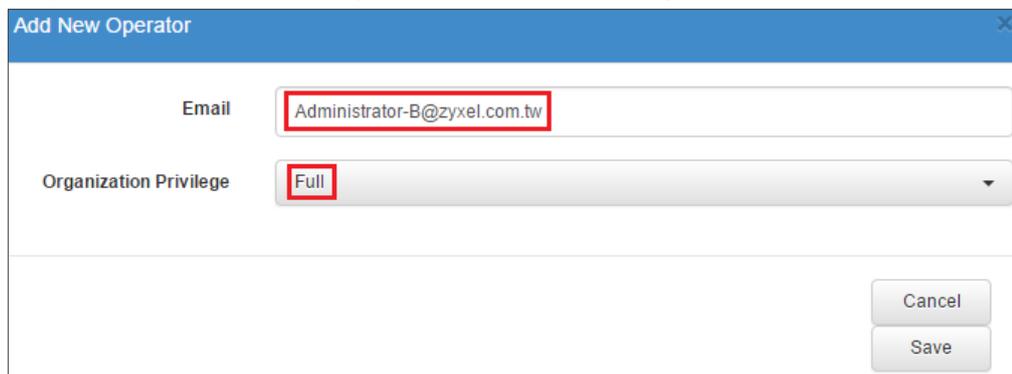
- 1 Log in to the Zyxel CNC, go to **Organization View > Operators**, click on the **Create Operator** button.

### Organization View > Operators



- 2 Provide **“Full”** organization privilege to accounts of administrators that are part of the MSP/VAR's organization. **“Full”** privilege gives the user account to add or remove operators from the organization.

### Organization View > Operators > Create Operator



- 3 Provide **“Read-Only”** organization privilege to accounts of local administrators in remote site upon requests. **“Read-Only”** organization privilege prohibits user account from adding or removing operators from the organization. Select how much authority to provide this account by selecting the appropriate site privilege.

## Organization View > Operators > Create Operator

💡 Note: Accounts with “Read-Only” organization privilege and “Read-Only” site privilege have limited functions and access. Restricted functions are greyed-out and will not be clickable.

💡 Accounts with “Read-Only” organization privilege and “Monitor-Only” site privilege can only check whether devices are currently in an **active** or **inactive** status.

## 2.2 Verify that Accounts are Granted Privilege

- 1 Go to **Organization Events**. Event should indicate that privilege of users have been added by the administrator.

### Organization Events

Organization Events

Add Organization/Site Organization View **Organization Events** Operators

Search Constraints: Legend

Event ID	Task ID	Severity	Time	Organization Name	Site Name	Event Name
451556	-[-][+]	NORMAL [+][+]	2016-05-24 13:05:30 UTC+08:00 [-][+]	CSO [+][+]	-[-][+]	Organization Event: orgUserAdd [+][+] Privilege of user local.administrator has been add for organization CSO by administrator-a
450668	-[-][+]	NORMAL [+][+]	2016-05-24 11:24:09 UTC+08:00 [-][+]	CSO [+][+]	-[-][+]	Organization Event: orgUserAdd [+][+] Privilege of user administrator-b has been add for organization CSO by administrator-a

## 2.3 What Could Go Wrong?

- 1 If CNC does not display the CNA, CNA may be receiving an incorrect **DHCP configuration**. Use the **ZON utility** through the local network to verify the DHCP configurations. IP address configurations should be able to provide CNA access to the Internet.

### ZON > IP Configuration

IP Configuration

ZyXEL

IP Configuration

IPv4 setting: DHCP

IP address: 192 . 168 . 1 . 34

Subnet mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 1 . 1

DNS1: 192 . 168 . 1 . 1

DNS2: 0 . 0 . 0 . 0

Info

System: cna100

Location:

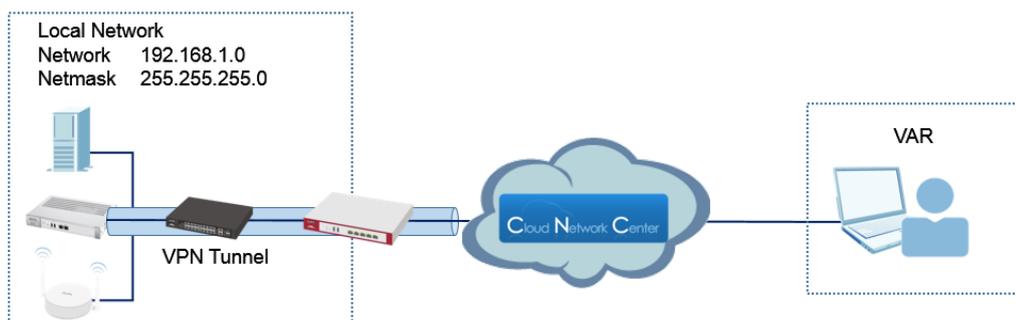
Device administrator password:

Apply Cancel

## 3 How to Provide Value Added Service using CNC

This example shows how to perform value added services to customer site through **Zyxel's Cloud Network Center (CNC)**. This example showcases the various value added services that CNC provides to remote sites.

**Figure 4** Applying Value Added Service to Remote Site



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110, GS1920-24HP, NWA5123-NI, and CNA100.

## 3.1 Discover Zyxel Devices in the Local Network

- 1 Log in to the Zyxel CNC, go to **Site View > Admin > Discover Nodes**, Click **Add New** to input the first and last IP address of the CNA100's network.

### Site View > Admin > Discover Nodes

The screenshot shows a modal dialog titled "Add Include Range to Discovery" with two input fields: "Begin IP Address" containing "192.168.1.1" and "End IP Address" containing "192.168.1.254". Below the dialog, the "Include Ranges" section contains a table with one row:

Begin IP Address	End IP Address	Action
192.168.1.0	192.168.1.255	

- 2 Clicking the **Discover** button initiates the discovery of Zyxel devices. Wait for a few seconds for CNC to register all devices.

### Site View > Admin > Discover Nodes

The screenshot shows the "Discover Nodes" page with a "Discover" button highlighted in red. The progress bar is at 100.00%. The "General settings" section shows a table with the following data:

Timeout (seconds)	Retry (times)	Action
1	0	

The "Include Ranges" section contains a table with one row:

Begin IP Address	End IP Address	Action
192.168.1.0	192.168.1.255	

- 3 Go to **Site View** to verify that all Zyxel devices are discovered.

## Site View

Site View						
3 Nodes						
Type	System Name	Interface	Status	Model	Firmware Version	Location
	Gateway	192.168.1.1		USG110	V4.15(AAPH.2)	
	Switch	192.168.1.10		GS1920-24HP	V4.30(AAOC.0)   09/16/2015	
	AccessPoint	192.168.1.35		NWA5123-NI	V4.20(AAHY.1)	Hsinchu,Taiwan

## 3.2 Schedule Firmware Upgrade

- 1 Log in to the Zyxel CNC, go to **Site > Admin > Device Firmware Upgrade > Add New Schedule**. Select which model on the **Model** tab and check the IP address of devices ready for firmware upgrade.

### Site > Admin > Device Firmware Upgrade > Add New Schedule

Add Firmware Upgrade Schedule
✕

Model: USG110

GS1920-24HP

NWA5123-NI

USG110

	Nodes	System Name	Firmware Version	Location
<input checked="" type="checkbox"/>	192.168.1.1	Gateway	V4.15(AAPH.2)	

- 2 Select the latest firmware on the **Official Firmware** tab.

**Site > Admin > Device Firmware Upgrade > Add New Schedule**

 **Note:** CNC automatically updates the **Official Firmware** list from the FTP servers. Administrators can upload a **Date Firmware** from their PC to the cloud server and select this firmware to upload to device.

- 3 Select **Upgrade Now** to initiate firmware upgrade immediately after clicking the **OK** button, or select **Scheduled Time** to initiate firmware upgrade on a specific date and time.

**Site > Admin > Device Firmware Upgrade > Add New Schedule**

- 4 Check the **Reboot after firmware upgrade** box and click the **OK** button.

**Site > Admin > Device Firmware Upgrade > Add New Schedule**

Reboot after firmware upgrade

Cancel

OK

 Note: Successfully uploading a firmware does not mean device is already using that firmware. New firmware is only applied after device successfully reboots.

- 5 Go to **Site > Admin > Device Firmware Upgrade > Add New Schedule**. An entry should display indicating a pending firmware upgrade schedule.

**Site > Admin > Device Firmware Upgrade**

Devices Firmware Upgrade Site View Outages Events Notices Admin

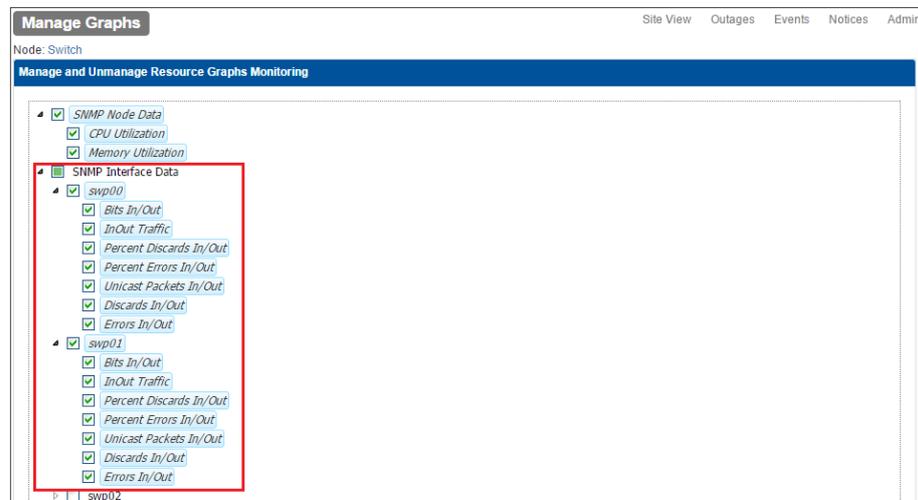
Add New Schedule

Firmware Upgrade Task List				
Time	Model	Interfaces	Target Firmware Information	Action
2016-05-27 22:30:00 UTC+08:00	USG110	192.168.1.1	V4.15(AAPH2)	 

### 3.3 Interpreting Graphs and Node Performance

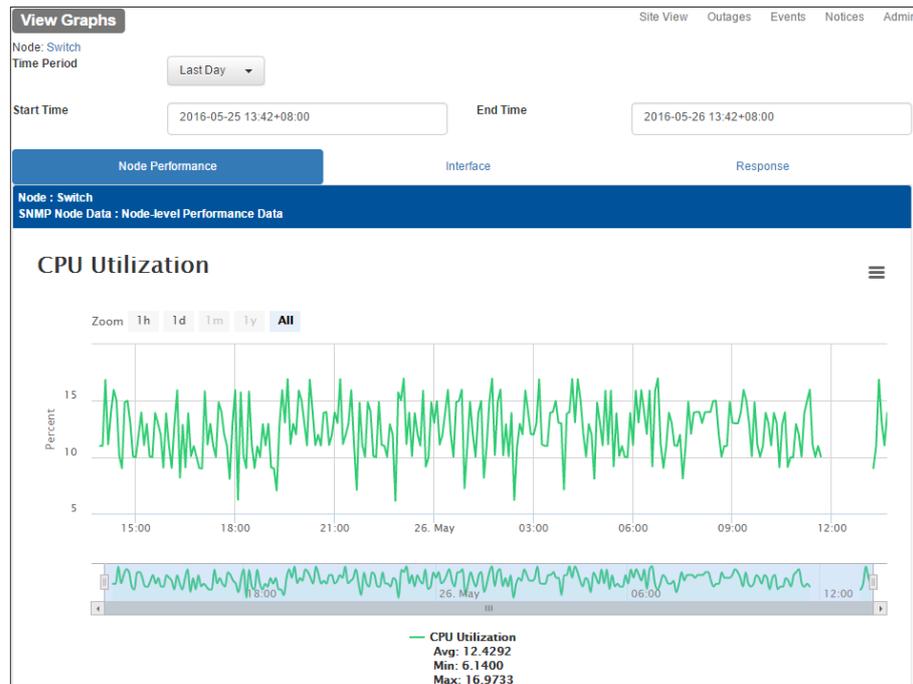
- 1 Log in to the Zyxel CNC, go to **Site > System Name > Manage Graphs**. Check **SNMP Interface Data** on interfaces to core network resources (ex: uplink port, servers).

#### Site > System Name > Manage Graphs



- 2 Go to **Site View > System Name > View Graphs** to view the various graphs and statistics.

## Site View > System Name > View Graphs



## 3.4 Receiving Email Notifications and Alerts during Link Failures

- 1 Log in to the Zyxel CNC, go to **Site View > Admin > Mail Groups**. Add the email addresses of site administrators for **Default Group**.

### Site View > Admin > Mail Groups > Settings

**Edit mail group**

Name:

Name	Status	Action
administrator-a@zyxel.com.tw	ON	
administrator-b@zyxel.com.tw	ON	
local.administrator@sitex.com	ON	

- 2 Go **Site View > Admin > Notifications**. Check the **Interface Down** notification and click the **Apply** button, afterwards.

### Site View > Admin > Notifications

Notifications			
Notification	Event	Mail Group	Action
<input type="checkbox"/> High CPU Threshold	Threshold Event: highCpuUtilThresholdExceeded	Default Group	
<input type="checkbox"/> High CPU Threshold Rearmed	Threshold Event: highCpuUtilThresholdRearmed	Default Group	
<input type="checkbox"/> High Memory Threshold	Threshold Event: highMemUtilThresholdExceeded	Default Group	
<input type="checkbox"/> High Memory Threshold Rearmed	Threshold Event: highMemUtilThresholdRearmed	Default Group	
<input type="checkbox"/> High Interface Utilization Threshold	Threshold Event: highIfUtilThresholdExceeded	Default Group	
<input type="checkbox"/> High Interface Utilization Threshold Rearmed	Threshold Event: highIfUtilThresholdRearmed	Default Group	
<input type="checkbox"/> High ICMP Response Time Threshold	Threshold Event: highIcmpRespThresholdExceeded	Default Group	
<input type="checkbox"/> High ICMP Response Time Threshold Rearmed	Threshold Event: highIcmpRespThresholdRearmed	Default Group	
<input type="checkbox"/> High SNMP Response Time Threshold	Threshold Event: highSnmpRespThresholdExceeded	Default Group	
<input type="checkbox"/> High SNMP Response Time Threshold Rearmed	Threshold Event: highSnmpRespThresholdRearmed	Default Group	
<input type="checkbox"/> Interface Up	Node Event: interfaceUp	Default Group	
<input checked="" type="checkbox"/> Interface Down	Node Event: interfaceDown	Default Group	

## 3.5 Backing-Up and Restoring Device Configurations

- 1 Log in to the Zyxel CNC, go to **Site View > Admin > User Name/Password > Add New Setting**. Backing-up and restoring configurations requires the device's valid username and password. Edit the Authentication User Setting by setting the device's IP address, valid username, and valid password. The default User Name/Password profile is "**admin/1234**" for all IP addresses.

### Site View > Admin > User Name/Password > Add New Setting

The screenshot shows a dialog box titled "Edit Authentication User Setting". It has a blue header bar with a close button (X). The main area contains four input fields: "First IP Address" with the value "192.168.1.1", "Last IP Address" with "192.168.1.1", "User Name" with "admin", and "Password" which is masked with ".....". At the bottom right, there are two buttons: "Cancel" and "OK".

- 2 Go to **Site View > Admin > Backup Time Frame Setting** to set the time CNC saves and stores the device's daily running configurations. Click the **Setting** button under the **Action** column to edit the time.

### Site View > Admin > Backup Time Frame Setting > Setting

The screenshot shows a dialog box titled "Set Backup Time". It has a blue header bar with a close button (X). The main area contains a "Time" label and a dropdown menu. The dropdown menu is open, showing three options: "08:00" (highlighted with a red box), "00:00 (UTC+08:00)", and "01:00 (UTC+08:00)". At the bottom right, there are two buttons: "Cancel" and "OK".

- 3 If you wish to manually back up a device's running configurations, go to **Site View > Device**. Click on the **Backup Now** button to save the device's running configurations to CNC.

## Site View > Device



- 4 To restore running configurations of devices, go to **Site View > Device > Restore Configure**. Click the **Restore** button under the Action column of the specific Backup Time to upload this configuration.

## Site View > Device > Restore Configure

The screenshot shows the 'Restore Configure' section of the ZyXel management interface. At the top right, there are navigation links: 'Site View', 'Outages', 'Events', 'Notices', and 'Admin'. Below these is the 'Node: Gateway' label. The 'Device Information' section displays the following details:

- IP address: 192.168.1.1
- Device model: USG110
- Firmware version: V4.15(AAPH.2)

The 'Backup Configuration' section contains a table with the following data:

Lock	Config ID	Backup Time	System Name	Location	Model	Firmware version	Action
<input type="checkbox"/>	471713	2016-05-25 08:01:55 UTC+08:00	Gateway		USG110	V4.15(AAPH.2)	<input type="checkbox"/>
<input type="checkbox"/>	431755	2016-05-24 08:01:55 UTC+08:00	Gateway		USG110	V4.15(AAPH.2)	<input type="checkbox"/>
<input type="checkbox"/>	276597	2016-05-23 08:01:55 UTC+08:00	Gateway		USG110	V4.15(AAPH.2)	<input type="checkbox"/>
<input type="checkbox"/>	274174	2016-05-22 08:01:55 UTC+08:00	Gateway		USG110	V4.15(AAPH.2)	<input type="checkbox"/>
<input type="checkbox"/>	271539	2016-05-21 08:01:55 UTC+08:00	Gateway		USG110	V4.15(AAPH.2)	<input type="checkbox"/>

The 'Restore' button (represented by a circular arrow icon) in the first row of the table is highlighted with a red box.

- Go to **Site View > Device**. Recent Events should show a **"configRestoreCompleted"** message to indicate configuration upload is successful.

## Site View > Device

Recent Events			
Event ID	Time	Severity	Description
477871	2016-05-26 13:16:16 UTC+08:00	NORMAL	Node Event: rescanCompleted
477870	2016-05-26 13:16:16 UTC+08:00	NORMAL	Discovery Event: nodeUpdate
477813	2016-05-26 13:16:08 UTC+08:00	NORMAL	Node Event: rescanStarted
477812	2016-05-26 13:16:08 UTC+08:00	NORMAL	Device Config Event: configRestoreCompleted
477860	2016-05-26 13:13:22 UTC+08:00	NORMAL	Device Config Event: configRestoreStarted
More...			

- Disconnect any non-uplink interface. CNC will send notifications to all accounts in the mail group. Access the mail box check if CNC has sent a notification.

**From:** no-reply@cnc.zyxel.com [mailto:no-reply@cnc.zyxel.com]  
**Sent:** Friday, May 27, 2016 2:31 PM  
**To:** CSO\_Switch  
**Subject:** ZyXEL CNC Notification : Interface Down

Dear [administrator-a@zyxel.com.tw](mailto:administrator-a@zyxel.com.tw) :

From Site : Site X

All services are down on interface 192.168.1.36 on node AccessPoint.

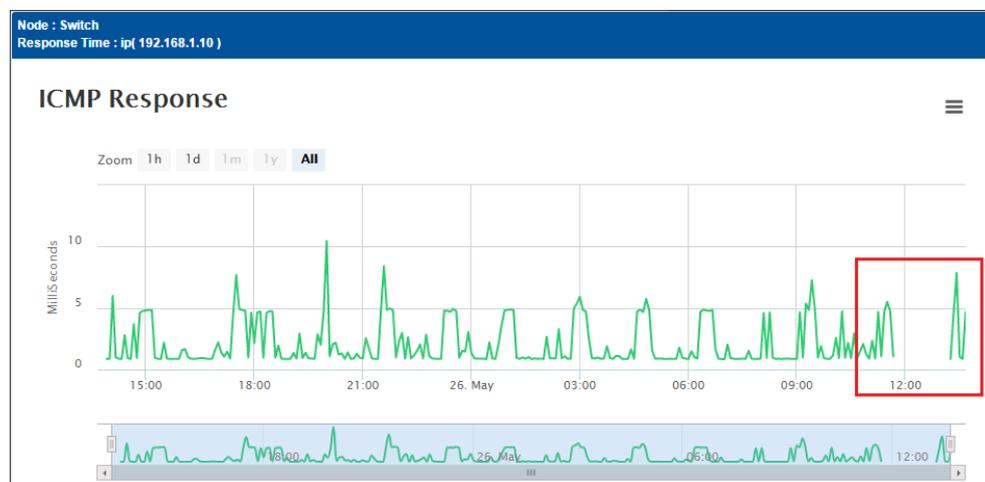
Best regards,  
 Cloud Network Center  
 ZyXEL Communications Corp.

**\*\*This is an automatically generated email, please do not reply\*\***

## 3.6 What Could Go Wrong?

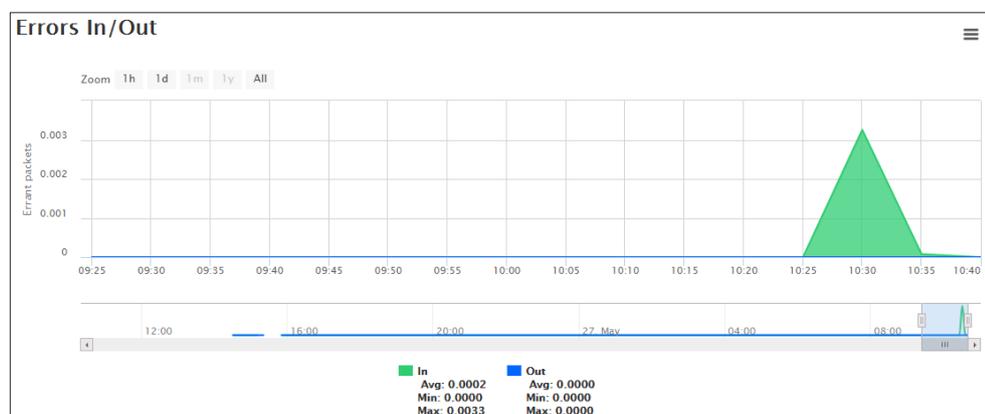
- 1 If the **ICMP Response** graph shows missing statistics, the following events may have occurred:
  - a. CNC lost connection to CNA.
  - b. CNA lost connection to this device.
  - c. Network is under the influence of a broadcast storm.

Site View > System Name > View Graphs > Response



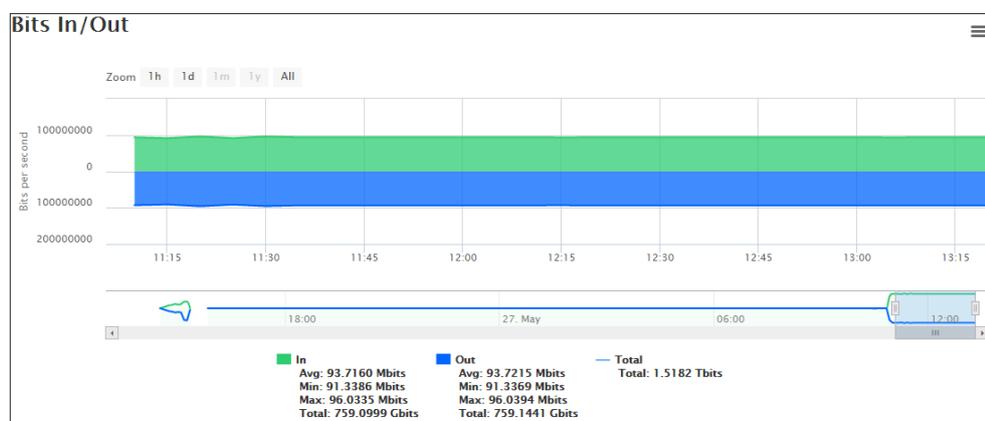
- 2 If the **Errors In/Out** interface graph shows any rise in counter, Ethernet cable may be damaged and require replacement.

Site View > System Name > View Graphs > Interface



- 3 If the Bits In/Out graph of an interface shows a cutoff, the following may have occurred:
  - a. Link bandwidth is in overcapacity. Consider load balancing traffic.
  - b. Network is under the influence of a Broadcast storm. Determine if network has connected loops.

### Site View > System Name > View Graphs > Interface



- 4 If the device Recent Events shows “**Device Config Event: configBackupFailed**”, make sure that CNC is using the correct user name and password in **Site View > Admin > User Name/Password > Add New Setting** for this device’s IP address.

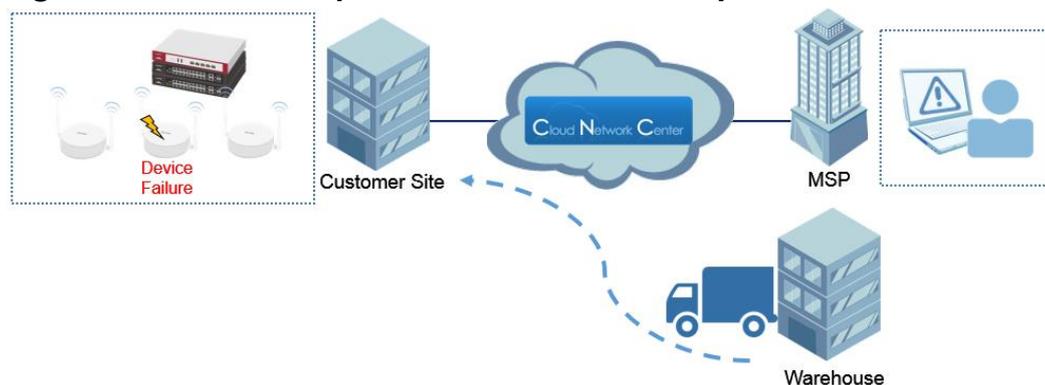
### Site View > Device

Recent Events			
Event ID	Time	Severity	Description
473879	2016-05-25 13:51:44 UTC+08:00	MAJOR	Device Config Event: configBackupFailed
473877	2016-05-25 13:51:15 UTC+08:00	MAJOR	Device Config Event: configBackupFailed
473876	2016-05-25 13:26:49 UTC+08:00	MAJOR	Device Config Event: configBackupFailed
473874	2016-05-25 13:22:03 UTC+08:00	NORMAL	Node Event: manageGraphsEdited
471541	2016-05-25 08:02:16 UTC+08:00	NORMAL	Device Config Event: configBackupCompleted
More...			

## 4 How to Replace and Recover Failed Devices

This example shows the general replacement process when a device is discovered to no longer able to power-on or perform any basic management or service on a remote site. The replacement process considers both **Centralized** and **Remote Site** management architecture. CNC provides a special feature called **Auto Restore** that allows convenient configurations and firmware recovery for replacement devices.

**Figure 5 Device Replacement and Recovery from MSP to Site**



## 4.1 Replacing Devices through Centralized Management

- 1 Log in to the Zyxel CNC, go to **Site View**. The damaged or malfunctioning device will be indicated as **offline** status.

### Site View

Type	System Name	Interface	Status	Model	Firmware Version	Location
Gateway	Gateway	192.168.1.1	Online	USG110	V4.15(AAPH.2)	
Switch	Switch	192.168.1.10	Online	GS1920-24HP	V4.30(AAOC.0)   09/16/2015	
AccessPoint	AccessPoint	192.168.1.35	Offline	NWA5123-NI	V4.20(AAHY.1)	Hsinchu,Taiwan

- 2 Go to **Site View > Device > Restore Configure**. Download the last good configuration by clicking on the **Download** button below the Action column.

### Site View > Device > Restore Configure

Lock	Config ID	Backup Time	System Name	Location	Model	Firmware version	Action
<input type="checkbox"/>	475165	2016-05-26 08:01:55 UTC+08:00	AccessPoint	Hsinchu,Taiwan	NWA5123-NI	V4.20(AAHY.1)	Refresh Download
<input type="checkbox"/>	471712	2016-05-25 08:01:55 UTC+08:00	AccessPoint	Hsinchu,Taiwan	NWA5123-NI	V4.20(AAHY.1)	Refresh Download
<input type="checkbox"/>	431754	2016-05-24 08:01:55 UTC+08:00	AccessPoint	Hsinchu,Taiwan	NWA5123-NI	V4.20(AAHY.1)	Refresh Download

- 3 Prepare replacement device in MSP office and upload the last good configuration. After uploading and saving configurations, deploy device back to remote site.



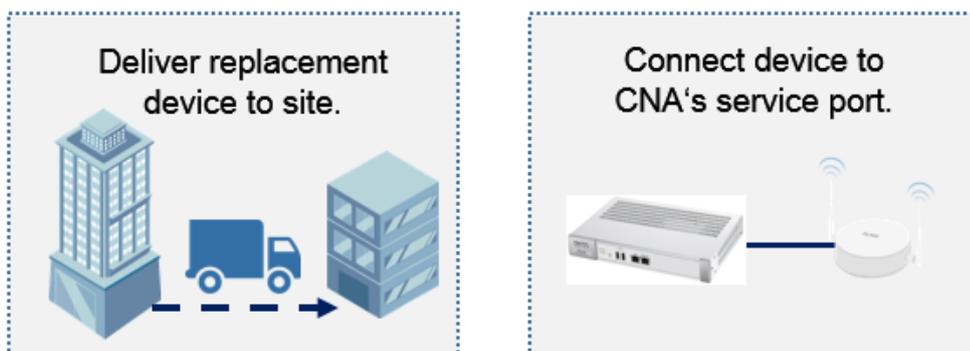
## 4.2 Replacing Devices through Remote Site Management

- 1 Log in to the Zyxel CNC, go to **Site View**. The damaged or malfunctioning device will be indicated as **offline** status.

### Site View

Site View						
Site View   Outages   Events   Notices   Admin						
3 Nodes						
Type	System Name	Interface	Status	Model	Firmware Version	Location
	Gateway	192.168.1.1		USG110	V4.15(AAPH.2)	
	Switch	192.168.1.10		GS1920-24HP	V4.30(AAOC.0)   09/16/2015	
	AccessPoint	192.168.1.35		NWA5123-NI	V4.20(AAHY.1)	Hsinchu, Taiwan

- 2 Deploy replacement device to remote site. Have the local administrator connect replacement device to the CNA's service port.



- 3 Log in to the Zyxel CNC, go to **Site View**. Click on the **System Name** of the device with the unique icon (🔧) that appears.

## Site View

Site View						
3 Nodes						
Type	System Name	Interface	Status	Model	Firmware Version	Location
	nwa5123-ni	0.0.0.0		NWA5123-NI	V4.20(AAHY.1)	Hsinchu,Taiwan
	Gateway	192.168.1.1		USG110	V4.15(AAPH.2)	
	Switch	192.168.1.10		GS1920-24HP	V4.30(AAOC.0)   09/16/2015	
	AccessPoint	192.168.1.35		NWA5123-NI	V4.20(AAHY.1)	Hsinchu,Taiwan

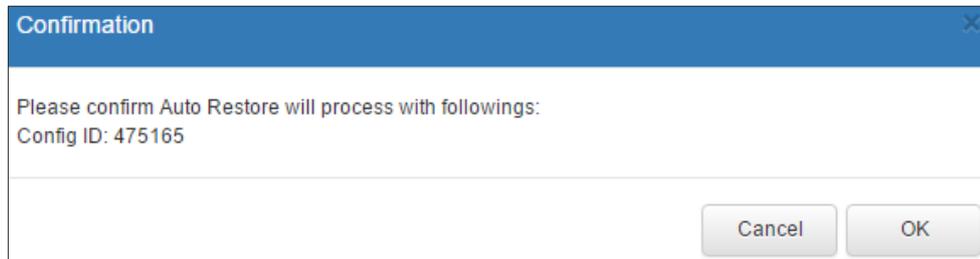
- 4 Click on the **Restore** icon of the last known good configuration under the Action column.

## Site View > Auto Restore Device

Auto Restore Device						
Auto restore will process the configuration restore and firmware upgrade in case the replacement device has older firmware than backup.						
Auto Restore Device Information						
IP address:	0.0.0.0					
Device model:	NWA5123-NI					
MAC address:	B0-B2-DC-6E-7E-BB					
Firmware version:	V4.20(AAHY.1)					
Status:						
Backup Configuration						
Status	Config ID	Backup time	System Name	Location	Firmware version	Action
	475165	2016-05-26 08:01:55 UTC+08:00	AccessPoint	Hsinchu,Taiwan	V4.20(AAHY.1)	
	471712	2016-05-25 08:01:55 UTC+08:00	AccessPoint	Hsinchu,Taiwan	V4.20(AAHY.1)	
	431754	2016-05-24 08:01:55 UTC+08:00	AccessPoint	Hsinchu,Taiwan	V4.20(AAHY.1)	

- 5 Click on the OK button to confirm that device will perform Auto Restore using the selected configurations and firmware. Wait for a few minutes until

## Site View > Auto Restore Device > Confirmation



- Go to Site > Events. Wait for **Event Name "autoRestoreCompleted"** message to appear. This will indicate that device has been successfully recovered and can now be disconnected from the CNA's service port.

## Site > Events

Events						
Event ID	Task ID	Severity	Time	System Name	Interface	Event Name
478042	- [ + ] [ - ]	NORMAL [ + ] [ - ]	2016-05-26 16:48:01 UTC+08:00 [ - ] [ + ]	AccessPoint [ + ] [ - ]	0.0.0.0 [ + ] [ - ]	Auto Restore Event: autoRestoreCompleted [ + ] [ - ]
Complete restoring procedure to AccessPoint with Config ID: 475165.						
478041	- [ + ] [ - ]	NORMAL [ + ] [ - ]	2016-05-26 16:44:15 UTC+08:00 [ - ] [ + ]	nwa5123-ni [ + ] [ - ]	0.0.0.0 [ + ] [ - ]	Auto Restore Event: autoRestoreStarted [ + ] [ - ]
Start restoring procedure to AccessPoint with Config ID: 475165.						
478093	- [ + ] [ - ]	NORMAL [ + ] [ - ]	2016-05-26 16:26:16 UTC+08:00 [ - ] [ + ]	- [ + ] [ - ]	- [ + ] [ - ]	Auto Restore Event: DeviceOnServicePortGained [ + ] [ - ]
Device on service port Gained.						

- 7 Contact the local administrator to swap the damaged or malfunctioning device with the replacement device.
  
- 8 If the malfunctioning or damaged device was using dynamic IP address configurations, go to **Site View > Admin > Discover Nodes**. Re-discover all the Zyxel devices in the site's local network.

## Site View > Admin > Discover Nodes

The screenshot shows the 'Discover Nodes' configuration page. At the top, there are 'Discover' and 'Cancel' buttons. Below is a progress bar showing 100.00%. The 'General settings' section contains a table for configuration parameters:

Timeout (seconds)	Retry (times)	Action
1	0	

The 'Specifics' section has an 'Add New' button and an 'IP Address' field with an 'Action' button. The 'Include Ranges' section has an 'Add New' button and a table for IP ranges:

Begin IP Address	End IP Address	Action
192.168.1.0	192.168.1.255	

The 'Exclude Ranges' section has an 'Add New' button and a table for IP ranges with columns for 'Begin IP Address', 'End IP Address', and 'Action'.

- 9 Go to **Site View**. If the replacement device is now indicated as an online device, click the System Name of the old entry.

## Site View

The screenshot shows the 'Site View' page with a table of 4 nodes. The table has the following columns: Type, System Name, Interface, Status, Model, Firmware Version, and Location. The row for the AccessPoint at 192.168.1.35 is highlighted with a red border.

Type	System Name	Interface	Status	Model	Firmware Version	Location
	Gateway	192.168.1.1		USG110	V4.15(AAPH.2)	
	Switch	192.168.1.10		GS1920-24HP	V4.30(AAOC.0)   09/16/2015	
	AccessPoint	192.168.1.35		NWA5123-NI	V4.20(AAHY.1)	Hsinchu,Taiwan
	AccessPoint	192.168.1.36		NWA5123-NI	V4.20(AAHY.1)	Hsinchu,Taiwan

- 10 After going to **Site View > Device**, click the Delete Node button to remove this node from the site device list.

## Site View > Device



 Note: Removing a node permanently removes the all the node's historic data. This includes the monitoring data, threshold status, and backup configurations.

## 4.3 What Could Go Wrong?

- 1 If the CNC does not display the device connected to the service port, go to **Organization View** to verify how many sites are being managed by this CNA. Auto Restore is disabled if the CNA is managing more than one site.

## Organization View

The screenshot shows the 'Organization View' interface with a search bar and an 'Auto Refresh' checkbox. Below is a table with the following data:

Site	Devices	Tags	CNA	Action
Site X	3 (Green), 0 (Yellow), 0 (Red)		Demo_2	Settings, Delete
Site Y	1 (Green), 0 (Yellow), 0 (Red)		Demo_2	Settings, Delete

The 'Demo\_2' entries in the CNA column are highlighted with a red rectangular box.

- 2 If the replacement device did not match the **Backup Configuration**'s firmware after undergoing auto restore, verify which firmware the replacement device was using. **Auto Restore** only updates firmware if the replacement device's firmware is older than the **Backup Configuration**.

## Site View > Auto Restore Device

**Auto Restore Device**
Site View Outages Events Notices Admin

Auto restore will process the configuration restore and firmware upgrade in case the replacement device has older firmware than backup.

**Auto Restore Device Information**

IP address: 192.168.1.11  
 Device model: GS3700-24  
 MAC address: 00-19-CB-00-00-02  
 Firmware version: V4.30(AAFY0\_20160506) 05/06/2016  
 Status:

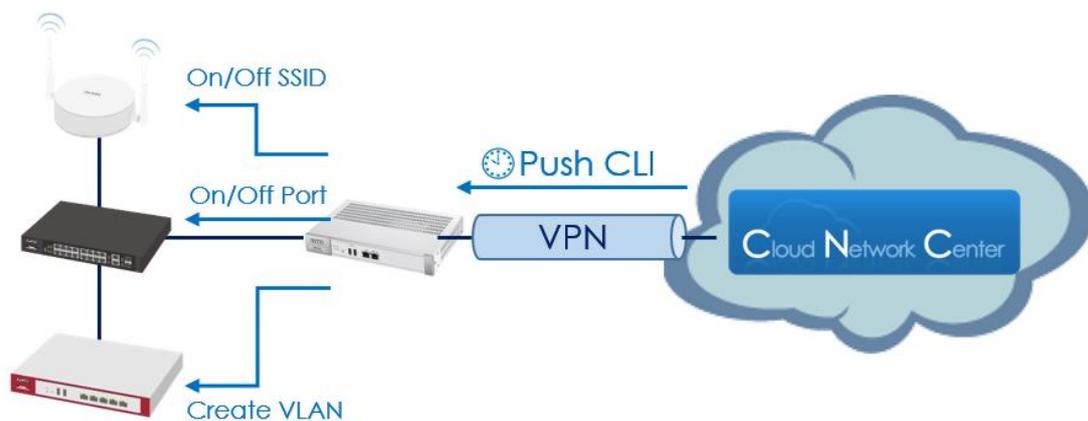
**Backup Configuration**

Status	Config ID	Backup time	System Name	Location	Firmware version	Action
	482115	2016-05-27 13:29:53 UTC+08:00	CoreSwitch		V4.30(AAFY0) 10/20/2015	

## 5 How to Auto-Provision Zyxel Devices Using CNC Push CLI

Push CLI utilizes the CNA to configure multiple devices using scripted CLI commands. CNC also allows Push CLI to run in a scheduled routine allowing for power saving or time-based service operations.

**Figure 6 CNC Auto-Provision through Push CLI**



**Note:** Push CLI cannot be used to auto-provision the **Zyxel Smart Managed Switches**. This is because the Zyxel Smart Managed Switches do not allow device configurations through CLI.

## 5.1 Configuring the Administrator Password for Switches

- 1 Log in to the Zyxel CNC, go to **Site View > Admin > Push CLI Commands** and select "Add New Schedule".

### Site View > Admin > Push CLI Commands

Status	Type	Trigger Time	Model	Interfaces	Expire Time	Action
COMPLETE	ONCE	2016-08-25 08:00:27 UTC+00:00	GS3700-48	192.168.172.44		
changePW						
COMPLETE	ONCE	2016-08-25 07:57:00 UTC+00:00	GS3700-48	192.168.172.44		
add vlan 10						
COMPLETE	ONCE	2016-08-25 07:46:47 UTC+00:00	GS3700-48	192.168.172.44		
vlan						
COMPLETE	ONCE	2016-08-25 07:31:21 UTC+00:00	XGS2210-28HP	192.168.172.179		

- 2 Select the Zyxel Switch **model** and **nodes** that will receive the CLI commands.

### Site View > Admin > Push CLI Commands > Add New Schedule

Selected 1/1 Nodes			
Interface	System Name	Firmware Version	Location
<input checked="" type="checkbox"/> 192.168.172.44	GS3700	V4.30(AAGA.0)   10/20/2015	192.168.172.44

- 3 Input the script into the **Commands** box.

**Site View > Admin > Push CLI Commands > Add New Schedule**

```
# Set timeout in seconds for furthering expect.
set timeout 60

# Wait till the keyword "GS3700#".
expect "GS3700#"

# Send the "config" command to enter config mode
send "conf\r"
# Wait till the keyword "GS3700(config)#".
expect "GS3700(config)#"
# Send the "admin-password <new password>" command to change
admin's password followed by enter key.
send "admin-password 12345\r"

expect "GS3700(config)#"
# Send the "exit" command to leave the config mode and followed by
an enter key.
send "exit\r"

expect "GS3700#"
# In order to close the SSH session properly, please remember to send
"exit" or equivalent command in the end of the script.
send "exit\r"
```

- 4 Select "Push Now" under the **Schedule Setting**. Afterwards, click the "OK" button.

## Site View > Admin > Push CLI Commands > Add New Schedule

Schedule Setting:

Push Now

Scheduled

Type Once ▾ Time   ⌚

Start Date   📅

Cancel
OK

- 5 The CLI output will produce the following:

```

GS3700# conf
GS3700(config)# admin-password 12345
GS3700(config)# exit
GS3700# exit
```

💡 Note: Do not forget to add or reconfigure the node's login credentials in **Site > Admin > User Name/Password** to the new credentials or else all authentication required services for this device will fail.

## 5.2 Creating and Configuring VLAN for Switches

- 1 Log in to the Zyxel CNC, go to **Site View > Admin > Push CLI Commands** and select “Add New Schedule”.

### Site View > Admin > Push CLI Commands

The screenshot shows the 'Push CLI Commands' interface. At the top, there is a navigation bar with 'Site View', 'Outages', 'Events', 'Notices', and 'Admin'. Below this is a 'Push CLI Commands' header with a sub-header 'Add New Schedule' highlighted in a red box. The main content is a 'Push Commands Task List' table with the following data:

Status	Type	Trigger Time	Model	Interfaces	Expire Time	Action
COMPLETE	ONCE	2016-08-25 08:00:27 UTC+00:00	GS3700-48	192.168.172.44		
changePW						
COMPLETE	ONCE	2016-08-25 07:57:00 UTC+00:00	GS3700-48	192.168.172.44		
add vlan 10						
COMPLETE	ONCE	2016-08-25 07:46:47 UTC+00:00	GS3700-48	192.168.172.44		
vlan						
COMPLETE	ONCE	2016-08-25 07:31:21 UTC+00:00	XGS2210-28HP	192.168.172.179		

- 2 Select the Zyxel Switch **model** and **nodes** that will receive the CLI commands.

### Site View > Admin > Push CLI Commands > Add New Schedule

The screenshot shows the 'Push Commands Schedule' configuration form. It includes the following fields:

- Model:** A dropdown menu with 'GS3700-48' selected, highlighted in a red box.
- Firmware:** A dropdown menu with 'ALL' selected.
- Nodes:** A section titled 'Selected 1/1 Nodes' containing a table with the following data:

	Interface	System Name	Firmware Version	Location
<input checked="" type="checkbox"/>	192.168.172.44	GS3700	V4.30(AAGA.0)   10/20/2015	192.168.172.44

- 3 Input the script into the **Commands** box.

**Site View > Admin > Push CLI Commands > Add New Schedule**

```
# Set timeout in seconds for furthering expect.
set timeout 60

# Wait till the keyword "GS3700#".
expect "GS3700#"

# Send the "config" command to enter config mode
send "config\r"
# Wait till the keyword "GS3700(config)#".
expect "GS3700(config)#"
# Send the "vlan <vlan ID>" command to create vlan followed by an
enter key.
send "vlan 10\r"
# Wait till the keyword "GS3700(config-vlan)#"
expect "GS3700(config-vlan)#"
# Send the "fixed <port ID>" command to add ports into the vlan
followed by an enter key.
send "fixed 1-10\r"
# Send the "untagged <port ID>" command to set the port as
untagged out port followed by an enter key.
send "untagged 1-10\r"
expect "GS3700(config-vlan)#"
# Send the "exit" command to leave the config-vlan mode and
followed by an enter key.
send "exit\r"
expect "GS3700(config)#"
# Send the "interface port-channel <port ID>" command to enter the
port config mode followed by an enter key.
send "interface port-channel 5-10\r"
expect "GS3700(config-interface)#"

```

```

expect "GS3700(config-interface)#"
# Send the "pvid <vlan ID>" command to add pvid into the port and
followed by an enter key.
send "pvid 10\r"

# Send the "exit" command to leave the port config mode and
followed by an enter key.
send "exit\r"

# Send the "exit" command to leave the config mode and followed by
an enter key.
send "exit\r"

expect "GS3700#"
# In order to close the SSH session properly, please remember to send
"exit" or equivalent command in the end of the script.
send "exit\r"

```

- 4 Select "Push Now" under the **Schedule Setting**. Afterwards, click the "OK" button.

**Site View > Admin > Push CLI Commands > Add New Schedule**

Schedule Setting:

Push Now

Scheduled

Type: Once

Time: [ ]

Start Date: [ ]

Cancel

OK

- The CLI output will produce the following:

```

GS3700#
GS3700# config
GS3700(config)# vlan 10
GS3700(config-vlan)# fixed 1-10
GS3700(config-vlan)# untagged 1-10
GS3700(config-vlan)# exit
GS3700(config)# interface port-channel 5-10
GS3700(config-interface)# pvid 10
GS3700(config-interface)# exit
GS3700(config)# exit
GS3700# exit
    
```

### 5.3 Scheduled PoE Port State for Switches

- Log in to the Zyxel CNC, go to **Site View > Admin > Push CLI Commands** and select "Add New Schedule".

#### Site View > Admin > Push CLI Commands

Push CLI Commands							Site View	Outages	Events	Notices	Admin
Add New Schedule											
Push Commands Task List											
Status	Type	Trigger Time	Model	Interfaces	Expire Time	Action					
COMPLETE	ONCE	2016-08-25 08:00:27 UTC+00:00	GS3700-48	192.168.172.44		 					
changePW											
COMPLETE	ONCE	2016-08-25 07:57:00 UTC+00:00	GS3700-48	192.168.172.44		 					
add vlan 10											
COMPLETE	ONCE	2016-08-25 07:46:47 UTC+00:00	GS3700-48	192.168.172.44		 					
vlan											
COMPLETE	ONCE	2016-08-25 07:31:21 UTC+00:00	XGS2210-28HP	192.168.172.179		 					

- 2 Select the Zyxel Switch **model** and **nodes** that will receive the CLI commands.

## Site View > Admin > Push CLI Commands > Add New Schedule

Push Commands Schedule
✕

Model: GS3700-48

---

Firmware: ALL

---

Nodes: Selected 1/1 Nodes

	Interface	System Name	Firmware Version	Location
<input checked="" type="checkbox"/>	<span style="border: 1px solid red; padding: 2px;">192.168.172.44</span>	GS3700	V4.30(AAGA.0)   10/20/2015	192.168.172.44

- 3 Input the script into the **Commands** box.

## Site View > Admin > Push CLI Commands > Add New Schedule

```
# Set timeout in seconds for furthering expect.
set timeout 60

# Wait till the keyword "XGS2210#".
expect "XGS2210#"

# Send the "config" command to enter config mode
send "config\r"
# Wait till the keyword "XGS2210(config)#".
expect "XGS2210(config)#"
# Send the "time-range <Name> <Type> <Range>" command to setup
PoE-scheduling time range.
send "time-range time1 periodic weekdays 08:00 to 17:00\r"
# Send the "pwr interface <port ID> time-range <time range name>"
command to setup PoE-scheduling time range.
```

```

send "pwr interface 1 time-range time1\r"
expect "XGS2210(config)#"
# Send the "exit" command to leave the config mode and followed by
an enter key.
send "exit\r"

expect "XGS2210#"
# In order to close the SSH session properly, please remember to send
"exit" or equivalent command in the end of the script.
send "exit\r"

```

- 4 Select "Push Now" under the **Schedule Setting**. Afterwards, click the "OK" button.

## Site View > Admin > Push CLI Commands > Add New Schedule

Schedule Setting:

Push Now

Scheduled

Type:  Time:

Start Date:

Cancel OK

- 5 The CLI output will produce the following:

```

XGS2210#
XGS2210# config
XGS2210(config)# time-range time1 periodic weekdays 08:00 to 17:00
XGS2210(config)# pwr interface 1 time-range time1
XGS2210(config)# exit
XGS2210# exit

```

## 5.4 Configuring the Administrator Password for Access Points

- 1 Log in to the Zyxel CNC, go to **Site View > Admin > Push CLI Commands** and select "Add New Schedule".

### Site View > Admin > Push CLI Commands

Status	Type	Trigger Time	Model	Interfaces	Expire Time	Action
COMPLETE	ONCE	2016-08-25 08:00:27 UTC+00:00	GS3700-48	192.168.172.44		
changePW						
COMPLETE	ONCE	2016-08-25 07:57:00 UTC+00:00	GS3700-48	192.168.172.44		
add vlan 10						
COMPLETE	ONCE	2016-08-25 07:46:47 UTC+00:00	GS3700-48	192.168.172.44		
vlan						
COMPLETE	ONCE	2016-08-25 07:31:21 UTC+00:00	XGS2210-28HP	192.168.172.179		

- 2 Select the Access Point **model** and **nodes** that will receive the CLI commands.

### Site View > Admin > Push CLI Commands > Add New Schedule

Model:

Firmware:

Nodes: **Selected 1/1 Nodes**

<input checked="" type="checkbox"/>	Interface	System Name	Firmware Version	Location
<input checked="" type="checkbox"/>	192.168.172.176	nwa5121-ni	V4.22(AAID.1)	

- 3 Input the script into the **Commands** box.

**Site View > Admin > Push CLI Commands > Add New Schedule**

```
# Set timeout in seconds for furthering expect.
set timeout 60

# Wait till the keyword "Router>".
expect "Router>"

# Send the "configure terminal" command to enter config mode
send "configure terminal\r"
# Wait till the keyword "Router(config)#".
expect "Router(config)#"
# Send the username command to change admin's password followed
by enter key.
send "username admin password 12345 user-type admin\r"

expect "Router(config)#"
# Send the "exit" command to leave the config mode and followed by
an enter key.
send "exit\r"

expect "Router#"
# In order to close the SSH session properly, please remember to send
"exit" or equivalent command in the end of the script.
send "exit\r"
```

- 4 Select “Push Now” under the **Schedule Setting**. Afterwards, click the “OK” button.

## Site View > Admin > Push CLI Commands > Add New Schedule

Schedule Setting:

Push Now

Scheduled

Type: Once

Time: [ ]

Start Date: [ ]

Cancel

OK

- 5 The CLI output will produce the following:

```
Router> configure terminal
Router(config)# username admin password 12345 user-type admin
Router(config)# exit
Router# exit
```

 Note: Do not forget to add or reconfigure the node's login credentials in **Site > Admin > User Name/Password** to the new credentials or else all authentication required services for this device will fail.

## 5.5 Creating an SSID for Access Points

- 1 Log in to the Zyxel CNC, go to **Site View > Admin > Push CLI Commands** and select "Add New Schedule".

### Site View > Admin > Push CLI Commands

Status	Type	Trigger Time	Model	Interfaces	Expire Time	Action
COMPLETE	ONCE	2016-08-25 08:00:27 UTC+00:00	GS3700-48	192.168.172.44		
changePW						
COMPLETE	ONCE	2016-08-25 07:57:00 UTC+00:00	GS3700-48	192.168.172.44		
add vlan 10						
COMPLETE	ONCE	2016-08-25 07:46:47 UTC+00:00	GS3700-48	192.168.172.44		
vlan						
COMPLETE	ONCE	2016-08-25 07:31:21 UTC+00:00	XGS2210-28HP	192.168.172.179		

- 2 Select the Access Point **model** and **nodes** that will receive the CLI commands.

### Site View > Admin > Push CLI Commands > Add New Schedule

Selected 1/1 Nodes	Interface	System Name	Firmware Version	Location
<input checked="" type="checkbox"/>	192.168.172.176	nwa5121-ni	V4.22(AAID.1)	

- 3 Input the script into the **Commands** box.

**Site View > Admin > Push CLI Commands > Add New Schedule**

```
# Set timeout in seconds for furthering expect.
set timeout 60

# Wait till the keyword "Router>".
expect "Router>"

# Send the "configure terminal" command to enter config mode
send "configure terminal\r"
# Wait till the keyword "Router(config)#".
expect "Router(config)#"
# Create SSID profile for "test" followed by enter key.
send "wlan-ssid-profile test\r"

# Wait till the keyword "Router(config-wlan-ssid test)#".
expect "Router(config-wlan-ssid test)#"
# Configure profile "test" to use SSID "test" followed by enter key.
send "ssid test\r"

# Send the "exit" command to leave the config mode and followed by
an enter key.
send "exit\r"

expect "Router(config)#"
# Send the "exit" command to leave the config mode and followed by
an enter key.
send "exit\r"

expect "Router#"
# In order to close the SSH session properly, please remember to send
"exit" or equivalent command in the end of the script.
send "exit\r"
```

- 4 Select "Push Now" under the **Schedule Setting**. Afterwards, click the "OK" button.

**Site View > Admin > Push CLI Commands > Add New Schedule**

Schedule Setting:

Push Now

Scheduled

Type: Once

Time: [ ]

Start Date: [ ]

Cancel

OK

- 5 The CLI output will produce the following:

```
Router> configure terminal
Router(config)# wlan-ssid-profile test
Router(config-wlan-ssid test)# ssid test
Router(config-wlan-ssid test)# exit
Router(config)# exit
Router# exit
```

## 5.6 Creating Scheduled SSID for Access Points

- 1 Log in to the Zyxel CNC, go to **Site View > Admin > Push CLI Commands** and select "Add New Schedule".

### Site View > Admin > Push CLI Commands

The screenshot shows the 'Push CLI Commands' interface. At the top, there is a navigation bar with 'Site View', 'Outages', 'Events', 'Notices', and 'Admin'. Below this is a button labeled 'Add New Schedule'. The main content area is titled 'Push Commands Task List' and contains a table with the following data:

Status	Type	Trigger Time	Model	Interfaces	Expire Time	Action
COMPLETE	ONCE	2016-08-25 08:00:27 UTC+00:00	GS3700-48	192.168.172.44		
changePW						
COMPLETE	ONCE	2016-08-25 07:57:00 UTC+00:00	GS3700-48	192.168.172.44		
add vlan 10						
COMPLETE	ONCE	2016-08-25 07:46:47 UTC+00:00	GS3700-48	192.168.172.44		
vlan						
COMPLETE	ONCE	2016-08-25 07:31:21 UTC+00:00	XGS2210-28HP	192.168.172.179		

- 2 Select the Access Point **model** and **nodes** that will receive the CLI commands.

### Site View > Admin > Push CLI Commands > Add New Schedule

The screenshot shows the 'Push Commands Schedule' form. It has a blue header with a close button. The form contains the following fields:

- Model:** A dropdown menu with 'NWA5121-NI' selected.
- Firmware:** A dropdown menu with 'ALL' selected.
- Nodes:** A section titled 'Selected 1/1 Nodes' containing a table with the following data:

<input type="checkbox"/>	Interface	System Name	Firmware Version	Location
<input checked="" type="checkbox"/>	192.168.172.176	nwa5121-ni	V4.22(AAID.1)	

- 3 Input the script into the **Commands** box.

**Site View > Admin > Push CLI Commands > Add New Schedule**

```
# Set timeout in seconds for furthering expect.
set timeout 60

# Wait till the keyword "Router>".
expect "Router>"

# Send the "configure terminal" command to enter config mode
send "configure terminal\r"
# Wait till the keyword "Router(config)#".
expect "Router(config)#"

# Create SSID profile for "test" followed by enter key.
send "wlan-ssid-profile test\r"
# Wait till the keyword "Router(config-wlan-ssid test)#".
expect "Router(config-wlan-ssid test)#"
# Enable SSID scheduling for profile "test" followed by enter key.
send "ssid-schedule\r"
# Disable "test" SSID during Saturdays and followed by enter key.
send "sat disable 00:00 00:00\r"
# Disable "test" SSID during Sundays and followed by enter key.
send "sun disable 00:00 00:00\r"

# Send the "exit" command to leave the config mode and followed by
an enter key.
send "exit\r"

expect "Router(config)#"
# Send the "exit" command to leave the config mode and followed by
an enter key.
send "exit\r"
```

```
expect "Router#"
# In order to close the SSH session properly, please remember to send
"exit" or equivalent command in the end of the script.
send "exit\r"
```

- 4 Select "Push Now" under the **Schedule Setting**. Afterwards, click the "OK" button.

**Site View > Admin > Push CLI Commands > Add New Schedule**

Schedule Setting:

Push Now

Scheduled

Type Once ▾ Time  ⌚

Start Date  📅

- 5 The CLI output will produce the following:

```
Router> configure terminal
Router(config)# wlan-ssid-profile test
Router(config-wlan-ssid test)# ssid-schedule
Router(config-wlan-ssid test)# sat disable 00:00 00:00
Router(config-wlan-ssid test)# sun disable 00:00 00:00
Router(config-wlan-ssid test)# exit
Router(config)# exit
Router# exit
```

## 5.7 Configuring Username/Password for Security Gateways

- 1 Log in to the Zyxel CNC, go to **Site View > Admin > Push CLI Commands** and select "Add New Schedule".

### Site View > Admin > Push CLI Commands

Status	Type	Trigger Time	Model	Interfaces	Expire Time	Action
COMPLETE	ONCE	2016-08-25 08:00:27 UTC+00:00	GS3700-48	192.168.172.44		
changePW						
COMPLETE	ONCE	2016-08-25 07:57:00 UTC+00:00	GS3700-48	192.168.172.44		
add vlan 10						
COMPLETE	ONCE	2016-08-25 07:46:47 UTC+00:00	GS3700-48	192.168.172.44		
vlan						
COMPLETE	ONCE	2016-08-25 07:31:21 UTC+00:00	XGS2210-28HP	192.168.172.179		

- 2 Select the Security Gateway **model** and **nodes** that will receive the CLI commands.

### Site View > Admin > Push CLI Commands > Add New Schedule

Model:

Firmware:

Nodes: **Selected 1/1 Nodes**

<input type="checkbox"/>	Interface	System Name	Firmware Version	Location
<input checked="" type="checkbox"/>	192.168.172.125	USG40W	V4.15(AALB.2)	

- 3 Input the script into the **Commands** box.

**Site View > Admin > Push CLI Commands > Add New Schedule**

```
# Set timeout in seconds for furthering expect.
set timeout 60

# Wait till the keyword "Router>".
expect "Router>"

# Send the "configure terminal" command to enter config mode
send "configure terminal\r"
# Wait till the keyword "Router(config)#".
expect "Router(config)#"
# Send the username command to change admin's password followed
by enter key.
send "username admin password 12345 user-type admin\r"

expect "Router(config)#"
# Send the "exit" command to leave the config mode and followed by
an enter key.
send "exit\r"

expect "Router#"
# In order to close the SSH session properly, please remember to send
"exit" or equivalent command in the end of the script.
send "exit\r"
```

- 4 Select “Push Now” under the **Schedule Setting**. Afterwards, click the “OK” button.

**Site View > Admin > Push CLI Commands > Add New Schedule**

Schedule Setting:

Push Now

Scheduled

Type: Once

Time: [ ]

Start Date: [ ]

Cancel

OK

- 5 The CLI output will produce the following:

```
Router> configure terminal
Router(config)# username admin password 12345 user-type admin
Router(config)# exit
Router# exit
```

Note: Do not forget to add or reconfigure the node's login credentials in **Site > Admin > User Name/Password** to the new credentials or else all authentication required services for this device will fail.

## 5.8 Creating a VLAN for Security Gateways

- 1 Log in to the Zyxel CNC, go to **Site View > Admin > Push CLI Commands** and select “Add New Schedule”.

### Site View > Admin > Push CLI Commands

The screenshot shows the 'Push CLI Commands' interface. At the top, there is a navigation bar with 'Site View', 'Outages', 'Events', 'Notices', and 'Admin'. Below this is a button labeled 'Add New Schedule'. The main content area is titled 'Push Commands Task List' and contains a table with the following data:

Status	Type	Trigger Time	Model	Interfaces	Expire Time	Action
COMPLETE	ONCE	2016-08-25 08:00:27 UTC+00:00	GS3700-48	192.168.172.44		
changePW						
COMPLETE	ONCE	2016-08-25 07:57:00 UTC+00:00	GS3700-48	192.168.172.44		
add vlan 10						
COMPLETE	ONCE	2016-08-25 07:46:47 UTC+00:00	GS3700-48	192.168.172.44		
vlan						
COMPLETE	ONCE	2016-08-25 07:31:21 UTC+00:00	XGS2210-28HP	192.168.172.179		

- 2 Select the Security Gateway **model** and **nodes** that will receive the CLI commands.

### Site View > Admin > Push CLI Commands > Add New Schedule

The screenshot shows the 'Push Commands Schedule' form. It includes the following fields and sections:

- Model:** A dropdown menu with 'USG40W' selected.
- Firmware:** A dropdown menu with 'ALL' selected.
- Nodes:** A section titled 'Selected 1/1 Nodes' containing a table with the following data:

<input checked="" type="checkbox"/>	Interface	System Name	Firmware Version	Location
<input checked="" type="checkbox"/>	192.168.172.125	USG40W	V4.15(AALB.2)	

- 3 Input the script into the **Commands** box.

**Site View > Admin > Push CLI Commands > Add New Schedule**

```
# Set timeout in seconds for furthering expect.
set timeout 60

# Wait till the keyword "Router>".
expect "Router>"

# Send the "configure terminal" command to enter config mode
send "configure terminal\r"
# Wait till the keyword "Router(config)#".
expect "Router(config)#"
# Create interface "vlan100" followed by enter key.
send "interface vlan100\r"
# Wait till the keyword "Router(config-if-vlan)#".
expect "Router(config-if-vlan)#"
# Process this interface in VID 100 followed by enter key.
send "vlan-id 100\r"
# Bind the VLAN to port "LAN1" followed by enter key.
send "port lan1\r"

# Send the "exit" command to leave the config mode and followed by
an enter key.
send "exit\r"

expect "Router(config)#"
# Send the "exit" command to leave the config mode and followed by
an enter key.
send "exit\r"
expect "Router#"
# In order to close the SSH session properly, please remember to send
"exit" or equivalent command in the end of the script.
send "exit\r"
```

- 4 Select “Push Now” under the **Schedule Setting**. Afterwards, click the “OK” button.

### Site View > Admin > Push CLI Commands > Add New Schedule

Schedule Setting:

Push Now

Scheduled

Type Once ▾ Time   ⌚

Start Date   📅

Cancel
OK

- 5 The CLI output will produce the following:

```
Router> configure terminal
Router(config)# interface vlan100
Router(config-if-vlan)# vlan-id 100
Router(config-if-vlan)# port lan1
Router(config-if-vlan)# exit
Router(config)# exit
Router# exit
```

## 5.9 Editing a VLAN IP Interface for Security Gateways

- 1 Log in to the Zyxel CNC, go to **Site View > Admin > Push CLI Commands** and select “Add New Schedule”.

### Site View > Admin > Push CLI Commands

The screenshot shows the 'Push CLI Commands' interface. At the top, there is a navigation bar with 'Site View', 'Outages', 'Events', 'Notices', and 'Admin'. Below this is a button labeled 'Add New Schedule'. The main content area is titled 'Push Commands Task List' and contains a table with the following data:

Status	Type	Trigger Time	Model	Interfaces	Expire Time	Action
COMPLETE	ONCE	2016-08-25 08:00:27 UTC+00:00	GS3700-48	192.168.172.44		
changePW						
COMPLETE	ONCE	2016-08-25 07:57:00 UTC+00:00	GS3700-48	192.168.172.44		
add vlan 10						
COMPLETE	ONCE	2016-08-25 07:46:47 UTC+00:00	GS3700-48	192.168.172.44		
vlan						
COMPLETE	ONCE	2016-08-25 07:31:21 UTC+00:00	XGS2210-28HP	192.168.172.179		

- 2 Select the Security Gateway **model** and **nodes** that will receive the CLI commands.

### Site View > Admin > Push CLI Commands > Add New Schedule

The screenshot shows the 'Push Commands Schedule' form. It includes the following fields and options:

- Model:** A dropdown menu with 'USG40W' selected.
- Firmware:** A dropdown menu with 'ALL' selected.
- Nodes:** A table titled 'Selected 1/1 Nodes' with the following data:

<input checked="" type="checkbox"/>	Interface	System Name	Firmware Version	Location
<input checked="" type="checkbox"/>	192.168.172.125	USG40W	V4.15(AALB.2)	

- 3 Input the script into the **Commands** box.

**Site View > Admin > Push CLI Commands > Add New Schedule**

```
# Set timeout in seconds for furthering expect.
set timeout 60

# Wait till the keyword "Router>".
expect "Router>"

# Send the "configure terminal" command to enter config mode
send "configure terminal\r"
# Wait till the keyword "Router(config)#".
expect "Router(config)#"
# Create interface "vlan100" followed by enter key.
send "interface vlan100\r"

# Wait till the keyword "Router(config-if-vlan)#".
expect "Router(config-if-vlan)#"
# Configure VLAN 100 interface with this IP address and mask followed
by enter key.
send "ip address 192.168.100.1 255.255.255.0\r"

# Send the "exit" command to leave the config mode and followed by
an enter key.
send "exit\r"

expect "Router(config)#"
# Send the "exit" command to leave the config mode and followed by
an enter key.
send "exit\r"
expect "Router#"
# In order to close the SSH session properly, please remember to send
"exit" or equivalent command in the end of the script.
send "exit\r"
```

- 4 Select “Push Now” under the **Schedule Setting**. Afterwards, click the “OK” button.

### Site View > Admin > Push CLI Commands > Add New Schedule

Schedule Setting:

Push Now
   
 Scheduled

Type Once ▾
Time  ⌄

Start Date  ≡

Cancel
OK

- 5 The CLI output will produce the following:

```

Router> configure terminal
Router(config)# interface vlan100
Router(config-if-vlan)# ip address 192.168.100.1 255.255.255.0
Router(config-if-vlan)# exit
Router(config)# exit
Router# exit
  
```

## 5.10 Verify that Push CLI is Successful

- 1 Log in to the Zyxel CNC, go to **Site View > Admin > Push CLI Commands** and select “Result” under the Action column of your Push CLI.

### Site View > Admin > Push CLI Commands

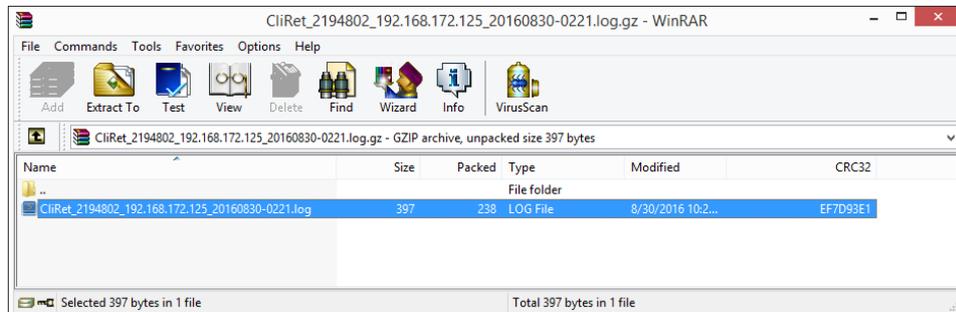
Push CLI Commands							Site View	Outages	Events	Notices	Admin
Add New Schedule											
Push Commands Task List											
Status	Type	Trigger Time	Model	Interfaces	Expire Time	Action					
COMPLETE	ONCE	2016-08-29 09:05:42 UTC+00:00	USG40W	192.168.172.125							
vlan 100, ip address											
COMPLETE	ONCE	2016-08-29 08:06:54 UTC+00:00	NWA5121-NI	192.168.172.176							
COMPLETE	ONCE	2016-08-29 06:59:37 UTC+00:00	NWA5121-NI	192.168.172.176							
COMPLETE	ONCE	2016-08-29 06:32:13 UTC+00:00	NWA5121-NI	192.168.172.176							
COMPLETE	ONCE	2016-08-29 06:28:56 UTC+00:00	NWA5121-NI	192.168.172.176							

- 2 Status should show “1“(complete). Click on the “Task ID” to track the CLI output.

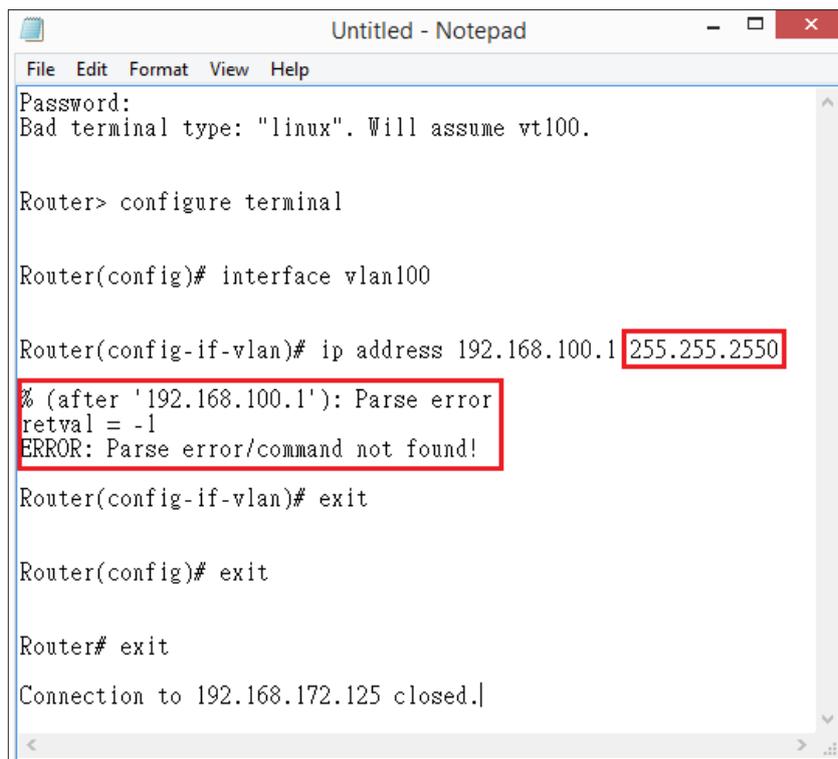
### Site View > Admin > Push CLI Commands > Results

Push CLI Result		
Update Time:	2016-08-30 02:10:17 UTC+00:00	
Time	Task ID	Status
2016-08-29 09:05:55 UTC+00:00	2188276	1  0
OK		

- Click the "Download Result" link. A .gz file will be downloaded.



- Extract and open the log to view if the CLI command was mistyped or invalid.



## 5.11 What Could Go Wrong?

- 1 If Push CLI Result shows “”, click on the “Task ID” to track the results.

### Site View > Admin > Push CLI Commands > Results

Push CLI Result		
Update Time: 2016-08-30 02:51:35 UTC+00:00		
Time	Task ID	Status
2016-08-30 02:51:07 UTC+00:00	2194790	 0  1
OK		

- 2 The Event Log may display the following Push CLI failures:

### Site View > Events

2194792	2194790 [+][-]	MAJOR [+][-]	2016-08-30 02:51:16 UTC+00:00 [<][>]	USG40W [+][-]	192.168.172.125 [+][-]	Push CLI Event: pushCLIFailed [+][-]
Push CLI: Check username/password is failed (error: Invalid user account or password) at node USG40W(192.168.172.125)						

For mismatched username/password, go to **Site View > Admin > User Name/Password** to edit or create new credentials.

### Site View > Events

2194924	2194879 [+][-]	MAJOR [+] [-]	2016-08-30 03:16:23 UTC+00:00 [<][>]	XGS2210-28HP [+][-]	192.168.172.179 [+][-]	Push CLI Event: pushCLIFailed [+][-]
Push CLI: Running script is failed (error: Error occurred while running script, visit log for more details.) at node XGS2210-28HP(192.168.172.179) <a href="#">Download Result</a>						

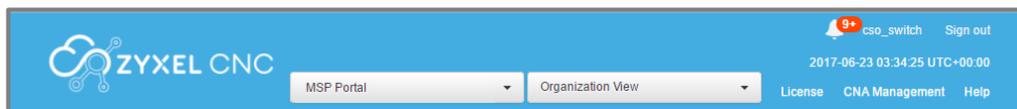
If Download Result shows “*ssh: connect to host 192.168.172.179 port 22: Connection refused*”, make sure that the device’s service port 22 (SSH) is not disabled.

## 6 How to Manage New Firmware Releases

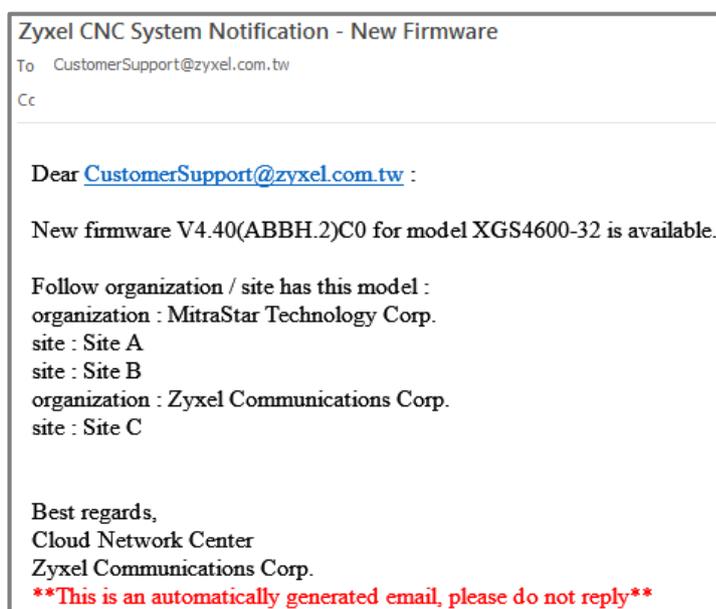
### 6.1 Receiving New Firmware Notifications

- 1 Log in to the Zyxel CNC. Look for the bell (🔔) icon at the top of the web page. The bell icon will show the number of new firmwares currently available.

#### MSP Portal

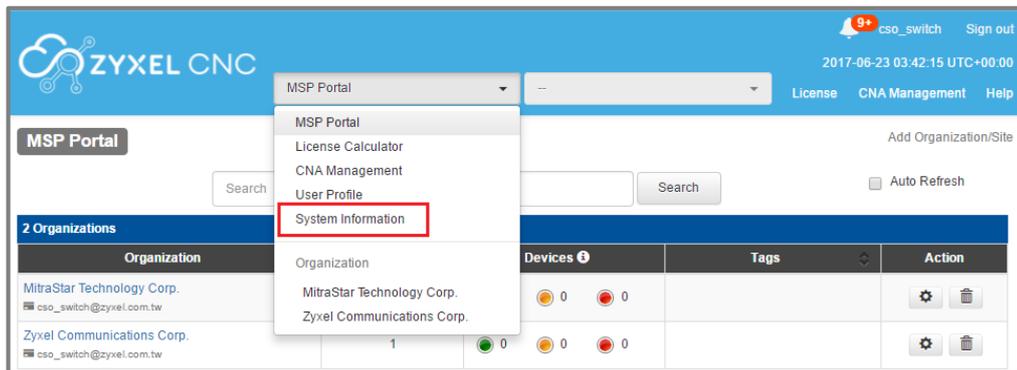


- 2 CNC sends New Firmware directly to your inbox. CNC also details the organizations and sites that contains the device model ready to upgrade this firmware version.



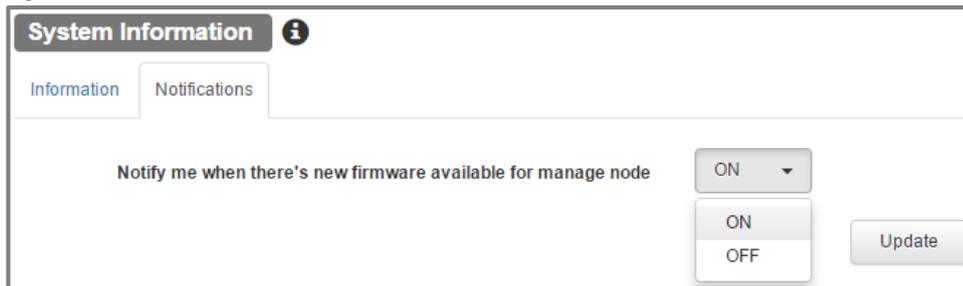
- 3 Select the  icon to automatically enter the System Information page. Alternatively, you can open the main selection window to enter the System Information page.

## MSP Portal



- 4 To prevent CNC from notifying your email account when a new firmware is available, go to **System Information > Notifications**. Select **OFF** and click **Update**.

## System Information > Notifications



## 6.2 Managing New Firmware Releases

- 1 Go to **System Information > Information**. The page shows firmwares that have been released. Click the  icon to view the firmware's release note.

### System Information > Information

System Information 			
Information		Notifications	
Date	Category	Information	Action
2017-05-22 UTC+00:00	New Firmware	New UAG5100 firmware V4.18(AAPN.0) is available	
2017-05-22 UTC+00:00	New Firmware	New UAG2100 firmware V4.18(AATD.0) is available	
2017-05-22 UTC+00:00	New Firmware	New UAG4100 firmware V4.18(AAIZ.0) is available	 
2017-05-17 UTC+00:00	New Firmware	New XS3700-24 firmware V4.30(AASS.0) is available	

- 2 Click the  icon to initiate firmware upgrade. A new window will appear. Select the organization and site. All device models for this corresponding firmware will be upgraded for this site. Click **OK**.

Select Organization and Site
✕

New firmware V4.18(AAIZ.0) is available for UAG4100 managed in the following organization/site. You can select the organization/site you would like to do firmware upgrade now. 

**Organization Name**

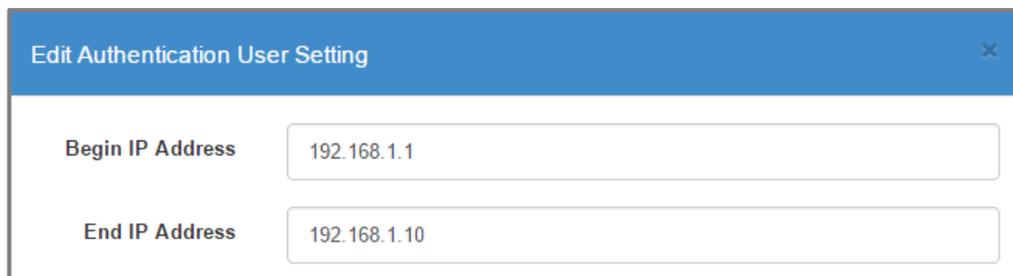
**Site Name**

## 7 How to Improve CNC Data Integrity

### 7.1 Enhancing Security through SNMPv3

- 1 Go to **Site View > Admin > SNMP Settings > Add New Setting**.  
Select the IP Range for nodes that will begin using SNMPv3.

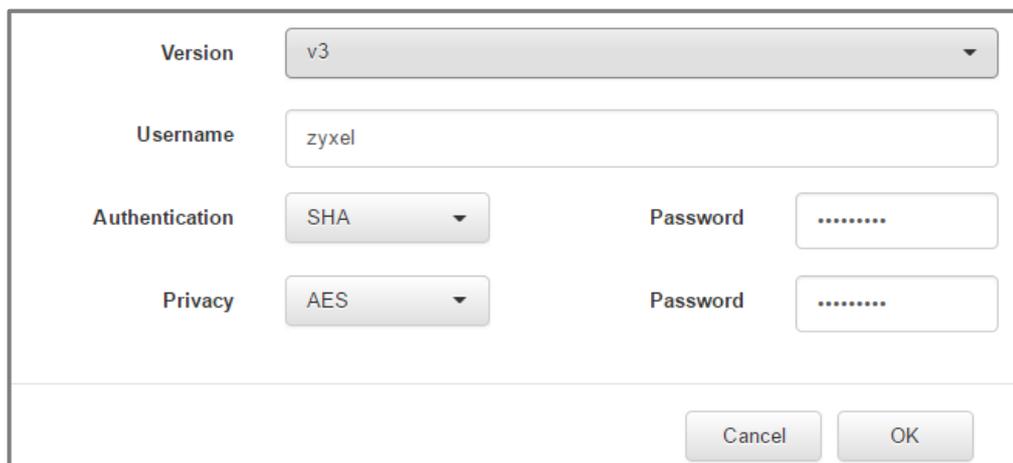
#### Site View > Admin > SNMP Settings > Add New Setting



The screenshot shows a dialog box titled "Edit Authentication User Setting" with a close button (X) in the top right corner. It contains two input fields: "Begin IP Address" with the value "192.168.1.1" and "End IP Address" with the value "192.168.1.10".

- 2 In the lower section of the window, select version **v3**. In this example, we will use Username "zyxel" while the Authentication and Privacy Password is "zyxel1234".

#### Site View > Admin > SNMP Settings > Add New Setting



The screenshot shows the same dialog box with additional configuration options. The "Version" dropdown menu is set to "v3". The "Username" field contains "zyxel". The "Authentication" dropdown is set to "SHA" and the "Privacy" dropdown is set to "AES". There are two "Password" fields, both containing masked characters (dots). At the bottom right, there are "Cancel" and "OK" buttons.

- 3 Access your Zyxel device. Configure your device SNMP settings similarly.

Example:

### XGS4600 Web GUI > Management > Access Control > SNMP

SNMP		<a href="#">Access Control</a>	<a href="#">Trap Group</a>	<a href="#">User</a>
<b>General Setting</b>				
Version	v3 ▼			
Get Community	public			
Set Community	public			
Trap Community	public			

### XGS4600 Web GUI > Management > Access Control > SNMP > User

User Information		<a href="#">SNMP Setting</a>		
Username	zyxel			
Security Level	priv ▼			
Authentication	SHA ▼	Password	zyxel1234	
Privacy	AES ▼	Password	zyxel1234	
Group	admin ▼			
<a href="#">Add</a> <a href="#">Cancel</a> <a href="#">Clear</a>				

 Note: SNMP settings differ across different Zyxel platforms. Consult the product user guide for detailed reference.

## 7.2 Verifying SNMPv3 Configurations

- 1 After configuring CNC and your Zyxel devices with your SNMPv3 user profile, go to **Site View**. Select the node using SNMPv3. Initiate a **Rescan**. The recent events window should show a “Node Event: rescanCompleted”.

### Site View > Device > Recent Events

Recent Events			
Event ID	Time	Severity	Description
3319483	2017-06-28 16:54:37 UTC+08:00	NORMAL	Node Event: rescanCompleted
3319482	2017-06-28 16:54:37 UTC+08:00	NORMAL	Discovery Event: nodeUpdate
3319538	2017-06-28 16:54:28 UTC+08:00	NORMAL	Node Event: rescanStarted
3319475	2017-06-28 16:46:27 UTC+08:00	NORMAL	Device Config Event: configBackupCompleted
3319529	2017-06-28 16:46:09 UTC+08:00	NORMAL	Device Config Event: configBackupStarted
<a href="#">More...</a>			

## 7.3 What May Go Wrong?

- 1 If CNC failed to rescan the node after using SNMPv3:

### Site View > Device > Recent Events

Recent Events			
Event ID	Time	Severity	Description
3319566	2017-06-28 17:01:06 UTC+08:00	MAJOR	Node Event: rescanFailed
3319564	2017-06-28 17:01:02 UTC+08:00	NORMAL	Node Event: rescanStarted
3319470	2017-06-28 16:41:15 UTC+08:00	NORMAL	Device Config Event: configBackupCompleted
3319469	2017-06-28 16:40:56 UTC+08:00	NORMAL	Node Event: rescanCompleted
3319468	2017-06-28 16:40:56 UTC+08:00	NORMAL	Discovery Event: nodeUpdate
<a href="#">More...</a>			

- a. Make sure that the CNA for this site is using the latest firmware version. You can go to **CNA Management** to verify and upgrade your CNA's firmware.
  - b. Make sure that the monitored device is also using SNMPv3 and using the correct usernames and passwords.
- 2** If some sites occasionally start reporting "***This action cannot be apply. CNA is Busy. Please retry again***" message after using SNMPv3, make sure that the CNA responsible for that site is not monitoring more than 125 SNMPv3 nodes.