



Application Note



Setting Up Multi-Site Networks on Nebula

Supported devices:

Nebula Security Gateway (NSG)
Nebula Switches (NSW) and NebulaFlex (Pro) Switches.
Nebula Access Points (NAPs) and NebulaFlex (Pro) APs

Nebula Cloud Networking and Management Solution

Introduction

When it comes to setting up and managing hundreds or sometimes even thousands of sites, automation is the key. Using automated tools to build and manage multiple networks will most certainly improve efficiency and alleviate workload, saving both time and money for businesses. This article addresses the important automated tools in [Nebula Control Center \(NCC\)](#) and its [Professional Pack](#) that can help IT admins to streamline mass deployment to multi-sites.

Expanding your network

Site Cloning

This is particularly useful for chain or franchise stores where each location has the same or similar network structure. After an organization is created and at least one site is already up and running in NCC, users can proceed to create new sites under the same organization. While creating the new site, users can utilize the **site-cloning** tool to easily clone **the site-wide device settings**.

1. Give the new site a name, select time zone and devices to add, if any.
2. Enable *Clone from [existing site]* in the *Configuration* section
3. Click on *Create site* button, and your new site will have the same site-wide settings as the existing one.

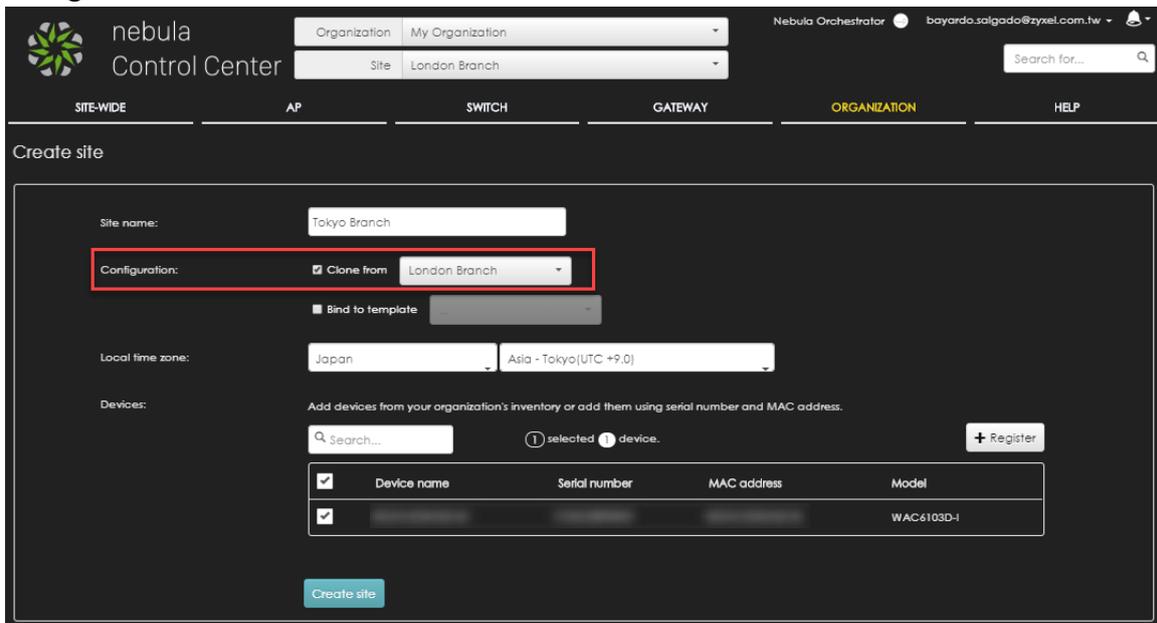


Figure 1 Site cloning enables users to clone site-wide device configurations from an existing site to a new site instantly.

The tool enables cloning of:

APs	Switches	Security Gateways
<ul style="list-style-type: none">• SSIDs• Captive portal themes• Site radio settings• Load balancing settings• Site Port settings.	<ul style="list-style-type: none">• Site IGMP settings• Voice VLANs• Radius policies• IP filtering rules• PoE schedule profiles	<ul style="list-style-type: none">• Content filtering• IDP• Anti-virus• Application patrol• Network server settings• Interfaces, Firewall rules, and policy routes as long as VPN is not enabled in the source site

Switch Cloning

Contrary to the AP and gateway settings that are mostly site-based, the settings for switch ports are device-based. The **switch-cloning** tool can be used to easily **replicate the switch settings between the same model devices across different sites**:

1. After the new site(s) have been cloned by using the site-cloning tool, users can proceed with the switch cloning located under the 'Organization' tab in the "Configuration management" page.
2. Use *From source device* to select the switch device that is already configured with the desired settings that you want to clone.
3. Use *To device(s)* to select the switch(es) that you want to update with the settings from the device selected in step 2. Note that only the switches of exactly the same model as the selected source device will be displayed in this list.
4. Click Clone and wait until the task is finished.

Note: It is highly recommended to first clone the site-wide switch settings, in this way the PoE and Radius policy profiles will also be used while cloning the switch port settings to the target devices.

The switch-cloning tool can be used to copy the following attributes between the same model devices:

- Switch port configuration
- Link aggregates
- STP bridge priority
- Mirrored ports
- Access policies
- Port PoE schedule
- Switch IGMP settings

You can leverage this feature to replicate the setting changes to all the devices across different sites under the same organization.

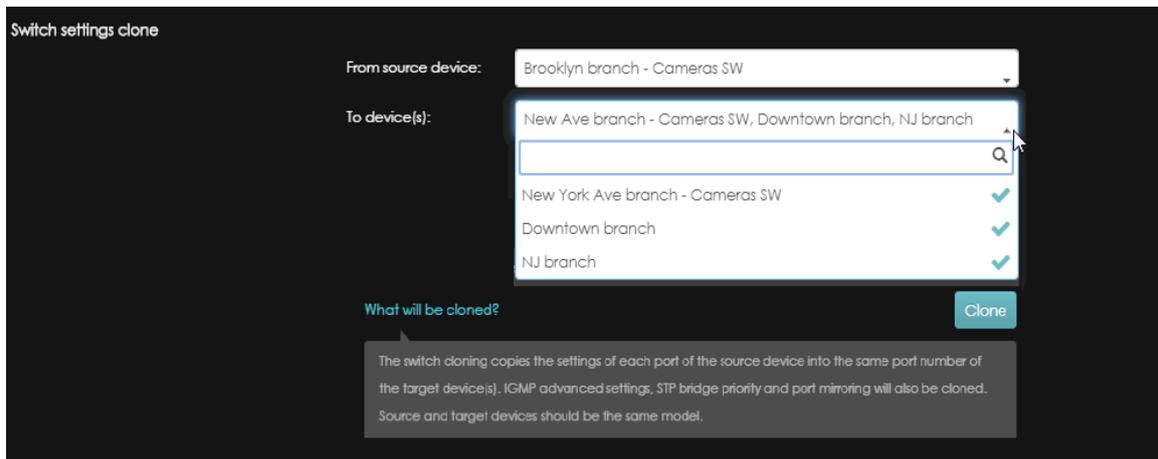


Figure 2 The switch-cloning tool can be used to replicate the settings between the same model devices

Save your stable network

Sites Backup and Restore

Once all the sites are deployed and the network is stable, users can make a backup of the settings of all sites under the same organization. **The backup creates a snapshot of all the sites' settings and stores it on the cloud. Users can restore the settings from an existing backup on per-site basis.**

To Backup:

1. Once the networks are performing as wanted, users can proceed to create a sites settings backup located under the 'Organization' tab in the "Configuration management" page.
2. In the *Site(s) settings* section, simply click the +Add button and give the backup a name.
3. Then, proceed to click the Save button and NCC will save the current settings of all the sites under this organization.

Note: user can create 3 backups as maximum. To generate more, it is necessary to delete an existing backup.

To Restore:

1. Once a backup has been created, the restore options will be shown on NCC. In order to restore to previous settings, select an existing backup in *Restore from backup* drop-down.
2. You could choose to perform a restoration to one or more sites, by selecting them in the *Restore to site(s)* drop-down.
3. Click the Restore button to perform the restoration to selected sites. The NCC will update those sites with the backed up settings, which at the same time will be pushed to the devices if applicable.
4. After performing setting restore, NCC will auto-generate one more backup which contains the settings right before doing the restoration, in case a rollback is needed.

Note: if an issue is encountered, the NCC default settings will be used. Devices added after the backup was performed will not be modify with per-device settings while doing the restoration.

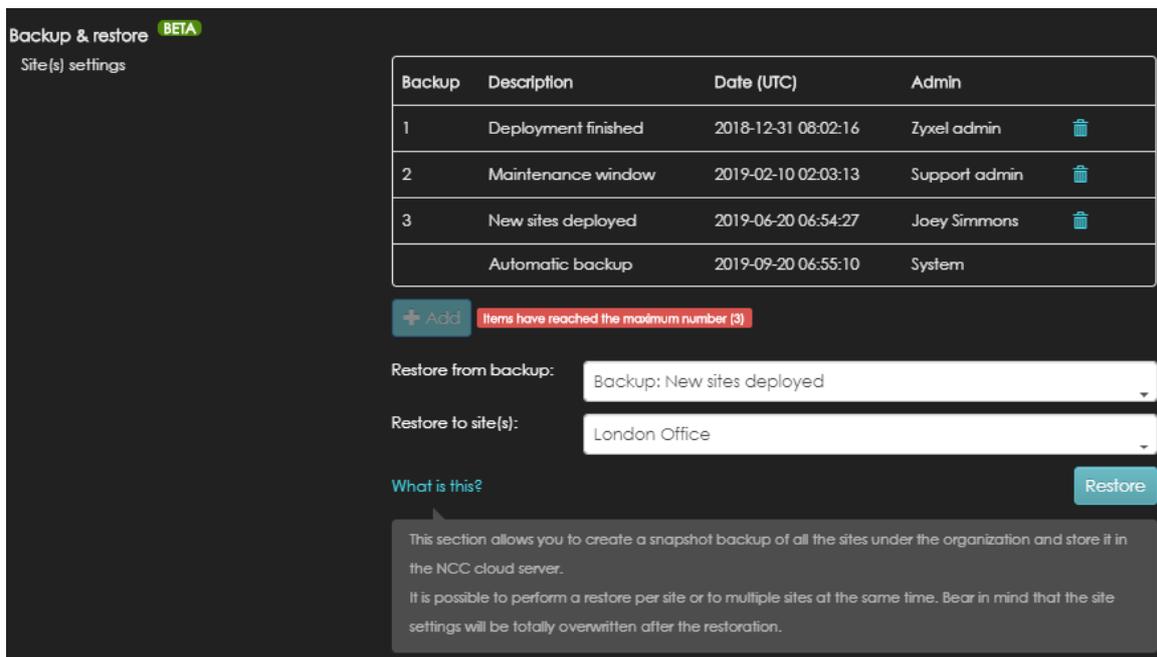


Figure 3 The backup and restore tool is particularly useful when doing a major change to the network to make sure users can go back to the previous settings if the change results in unstable network performance.

Switch Backup

Similar to switch cloning, the switch requires a dedicated backup and restore tool, which is especially useful for RMA scenarios. You can perform **a backup of the original device** before sending it back to the manufacturer and **apply the same configuration to the replacement device** as soon as you receive it, to minimize network downtime.

In addition, **one switch backup can also be applied to many devices** for mass deployment, just like the switch cloning tool.

To Backup:

1. Before removing the original device from the site, the settings can be first backed up in the "Configuration management" page located under the 'Organization' tab.
2. In the *Switch settings* section, simply click the +Add button, select the device and give the backup a name.
3. Then, proceed to click the Save button and NCC will save the current settings of the selected device.

Note: only one backup per device is allowed.

To Restore:

1. After the replacement device has been registered into the site, you could proceed to do a restoration of the backed up settings.
2. The restore options will be shown on NCC once a backup has been created. Select an existing backup in *Restore from backup* drop-down.
3. Now select the replacement device(s) in the *Restore to device(s)* drop-down. Note that original and replacement device(s) must be the exact same model.
4. Click the Restore button to perform the restoration to selected devices. Once completed, your replacement devices will be ready to use.

Note: switch port names and tags are restored, but switch device name a tags will not be included.

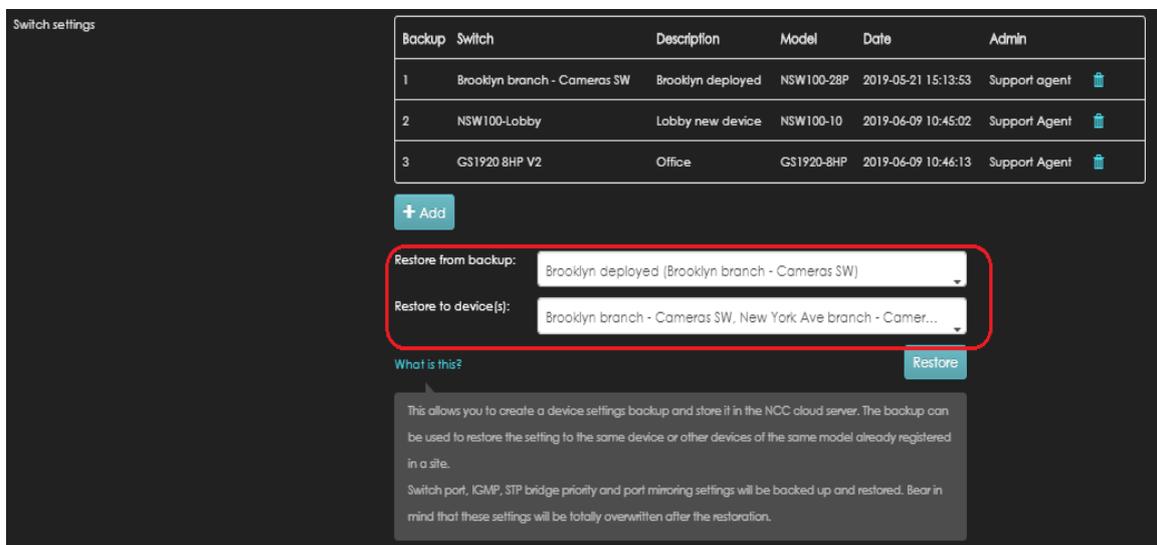


Figure 4 Users can perform a backup of a switch and restore the settings to many devices of the same model.

Keeping your networks updated and synchronized

Synchronization

The synchronization tool, part of the Organization Configuration management, provides users with an easy way **to synchronize some of the settings** that might change from time to time, such as:

- Site-wide general settings: Device local credentials, Captive portal re-authentication times, and SNMP.
- SSID settings: Authentication methods, Captive portal themes, and access policies.

If the credentials used while connecting through SSH to the Nebula devices need to be updated across all the sites due to security concern, you simply need to:

1. Change it in one of the sites.
2. Access the Synchronization menu section in the "Configuration management" page.
3. Select Settings as Site-wide general setting, and the site that has been already modified as a source site.
4. Select the sites that need to be synchronized, and finally click the Sync button, which will update all the selected sites simultaneously.

In the case that one of the SSID's password, authentication method or captive portal theme needs to be updated or you need to enable a completely new SSID in the networks, the process is similar, just need to set Settings to "SSIDs".

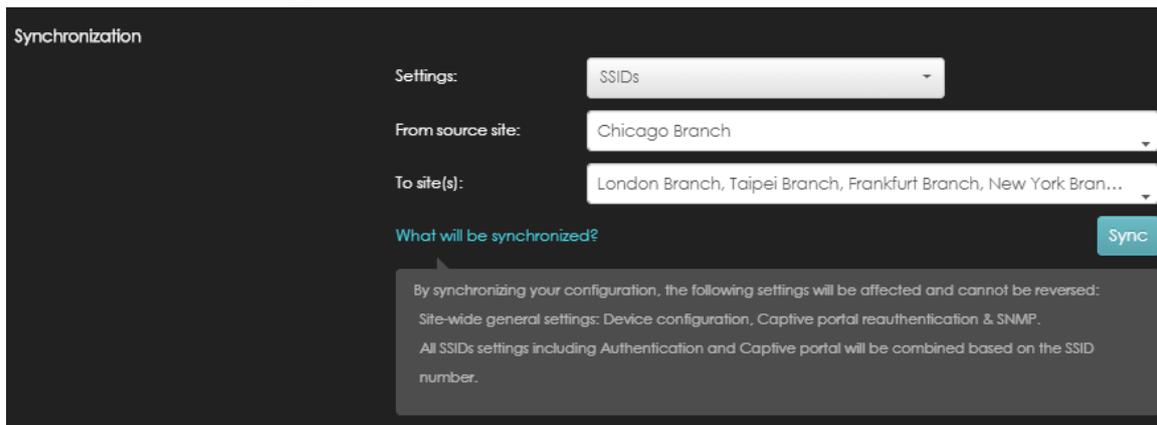


Figure 5 The synchronization tool provides users with an easy way to sync setting, like SSIDs across different sites.

Configuration Template – (Switch global settings)

The configuration template is another tool that will **help maintain multiple sites automatically synced while applying setting changes to a master template**. Once your networks are deployed, you could create a template using one of the site's configuration as a base, and bind all the sites that you need to maintain to the template.

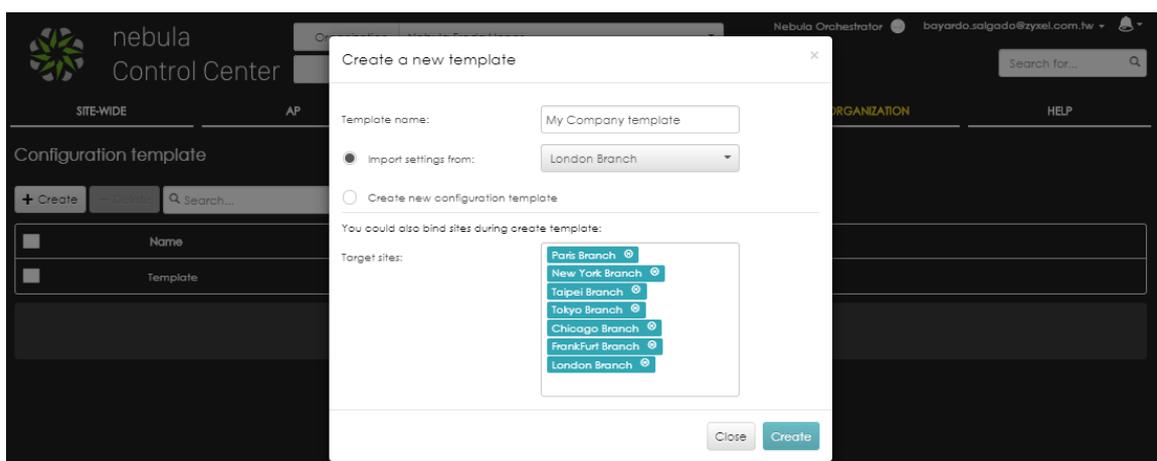


Figure 6 Creating a new template allows to copy settings from an existing site and bind the needed sites.

Once the sites are bound, every change made on the template will be replicated to these sites. A **local override option** can be enabled on a bound site, allowing to update its settings, and not applying further changes made on the template until the override is disabled again.

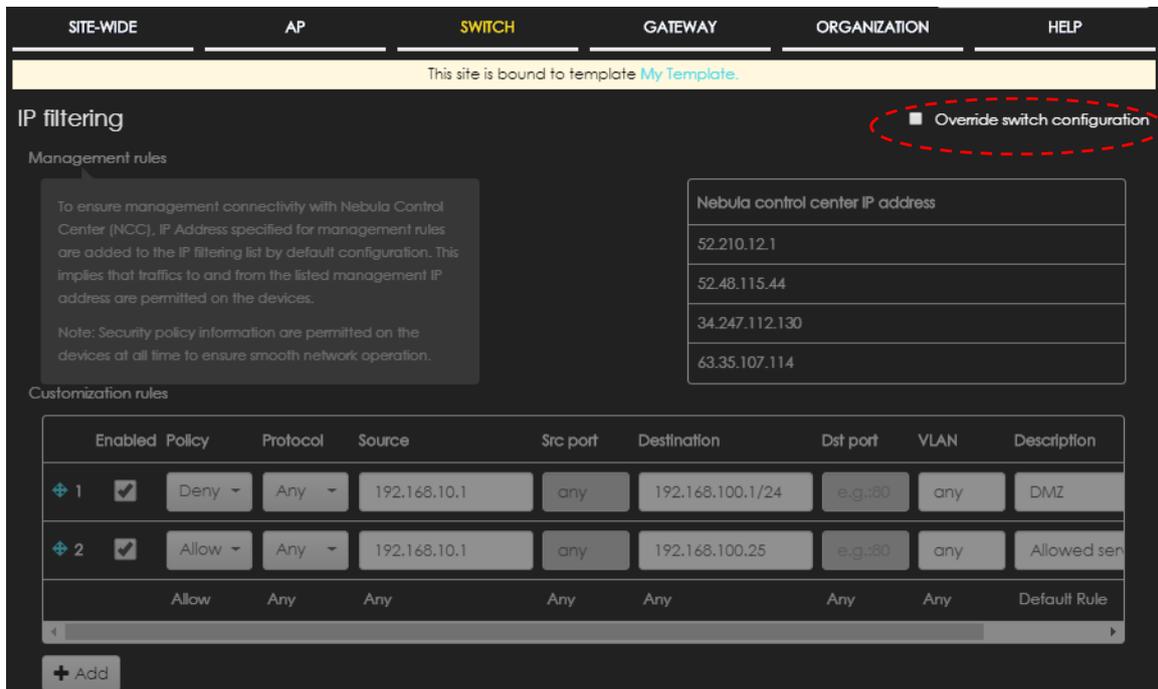


Figure 7 While a site is bound and follows a template configuration, its settings are grayed-out. Override can be enabled to allow settings modification, not following the template if any change is applied.

At the time of writing, the Configuration template supports switch common settings only, therefore, it is recommended to use if only switch setting changes are needed. Updating the IP filtering rules, PoE schedule profiles or voice VLANs can be easily modified on the template, and instantly sync to all the bound sites without further user intervention.

The configuration template scope will be expanded to cover more settings including Site-wide, APs, Switch ports and Gateways, in the coming releases.

ZYXEL

Your Networking Ally