# Install Replacement Devices

*For supported software information, click here.*

If a bare-metal hardware device, a virtual machine (VM), or cloud device that you have already configured fails or is faulty, or if you want to update hardware to add more CPU cores or RAM for higher throughput, you return the device by requesting an RMA for it. In an SD-WAN infrastructure deployment, the Director node maintains a copy of the SD-WAN branch configuration, so you can re-apply the branch configuration to the replacement device.

This article describes the steps to perform after you have received the replacement devices.

For information about the hardware RMA procedure, see How To Return Hardware.

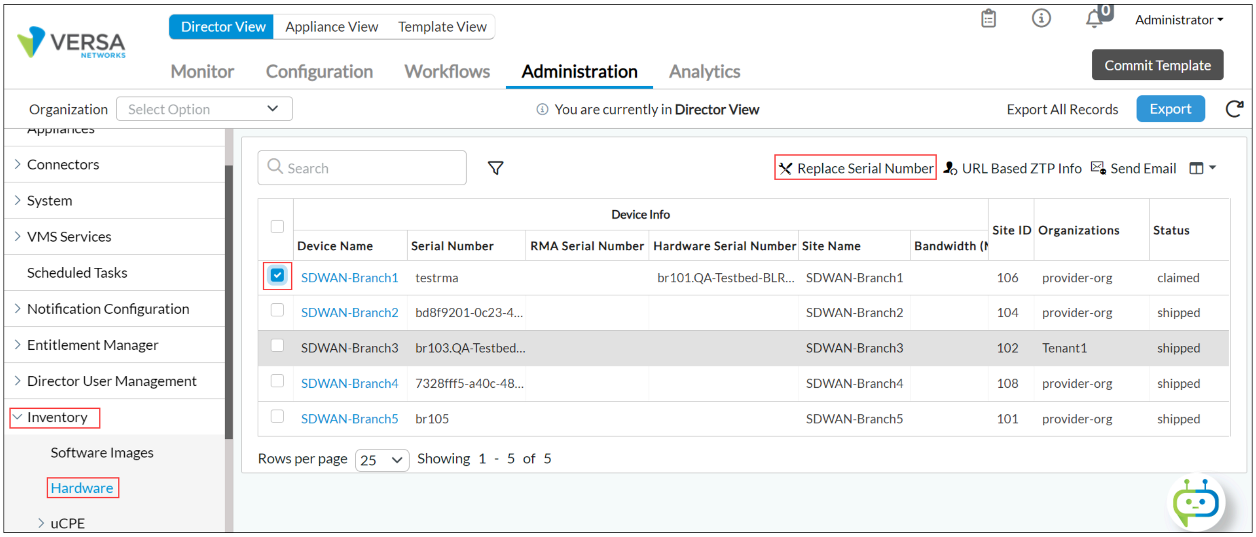
## Install New Hardware Devices after RMA

A replacement hardware device has a different serial number. To use the replacement device, you must associate the new serial number with the branch device's configuration. Then, you use zero-touch provisioning (ZTP) to activate the branch device.

The procedure in this section applies to devices running Releases 21.2.3 or later regardless of whether password encryption is enabled. For devices on which password encryption is enabled, the individual encryption keys and the replacement device's key can decrypt the passwords in the device's configuration that is stored on the Director node. The procedure in this section also applies to devices running earlier software releases on which password encryption is not enabled. If password encryption is enabled, follow the procedure in Redeploy VOS Devices Running Release 20.2 through Release 21.2.2 after RMA, below.

To associate the replacement device's serial number with the branch device's configuration:

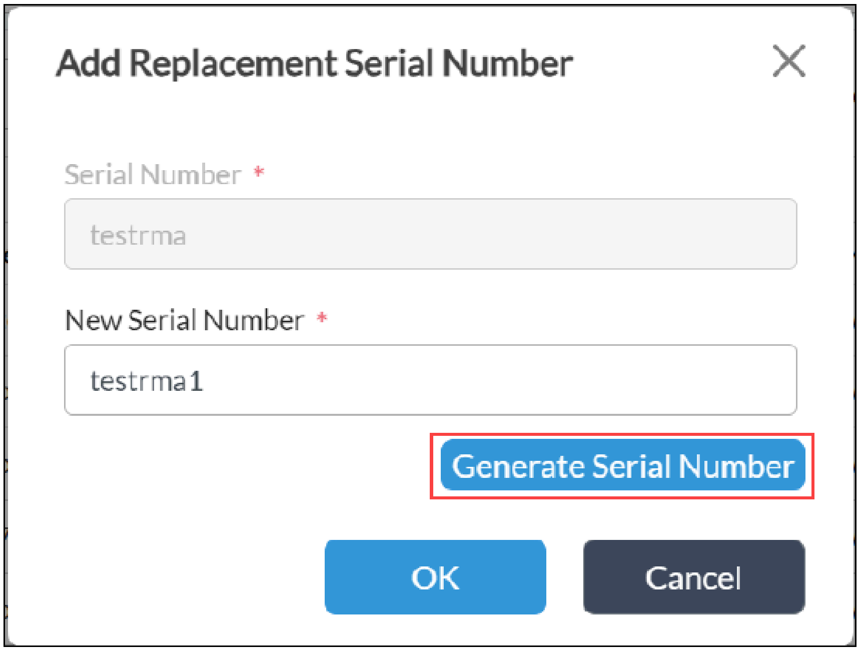
1. In Director view, select the Administration tab in the top menu bar.
2. Select Inventory > Hardware in the left menu bar.
3. Select the device, and then click the ✕ Replace Serial Number icon.



| □ | Device Info | | | | | | Site ID | Organizations | Status |
|---|---|---|---|---|---|---|---|---|---|
| | Device Name | Serial Number | RMA Serial Number | Hardware Serial Number | Site Name | Bandwidth (M | | | |
| ☑ | SDWAN-Branch1 | testrma | | br101.QA-Testbed-BLR... | SDWAN-Branch1 | | 106 | provider-org | claimed |
| □ | SDWAN-Branch2 | bd8f9201-0c23-4... | | | SDWAN-Branch2 | | 104 | provider-org | shipped |
| □ | SDWAN-Branch3 | br103.QA-Testbed... | | | SDWAN-Branch3 | | 102 | Tenant1 | shipped |
| □ | SDWAN-Branch4 | 7328fff5-a40c-48... | | | SDWAN-Branch4 | | 108 | provider-org | shipped |
| □ | SDWAN-Branch5 | br105 | | | SDWAN-Branch5 | | 101 | provider-org | shipped |

Rows per page 25 Showing 1 - 5 of 5

4. In the Add Replacement Serial Number popup window, enter the serial number of the new device or click Generate Serial Number.

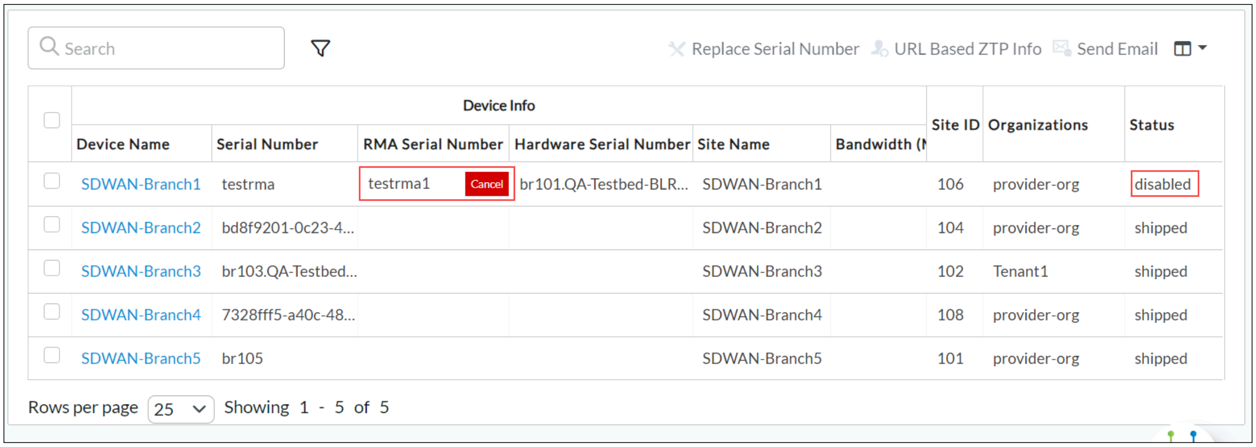


Add Replacement Serial Number

Serial Number * testrma

New Serial Number * testrma1

5. Click OK. In the Device Information group of fields, the RMA Serial Number field displays the serial number, and the status of the device shows as Disabled. To cancel the replacement serial number, click the Cancel button.



| □ | Device Info | | | | | | Site ID | Organizations | Status |
|---|---|---|---|---|---|---|---|---|---|
| | Device Name | Serial Number | RMA Serial Number | Hardware Serial Number | Site Name | Bandwidth (I | | | |
| □ | SDWAN-Branch1 | testrma | testrma1 Cancel | br101.QA-Testbed-BLR... | SDWAN-Branch1 | | 106 | provider-org | disabled |
| □ | SDWAN-Branch2 | bd8f9201-0c23-4... | | | SDWAN-Branch2 | | 104 | provider-org | shipped |
| □ | SDWAN-Branch3 | br103.QA-Testbed... | | | SDWAN-Branch3 | | 102 | Tenant1 | shipped |
| □ | SDWAN-Branch4 | 7328fff5-a40c-48... | | | SDWAN-Branch4 | | 108 | provider-org | shipped |
| □ | SDWAN-Branch5 | br105 | | | SDWAN-Branch5 | | 101 | provider-org | shipped |

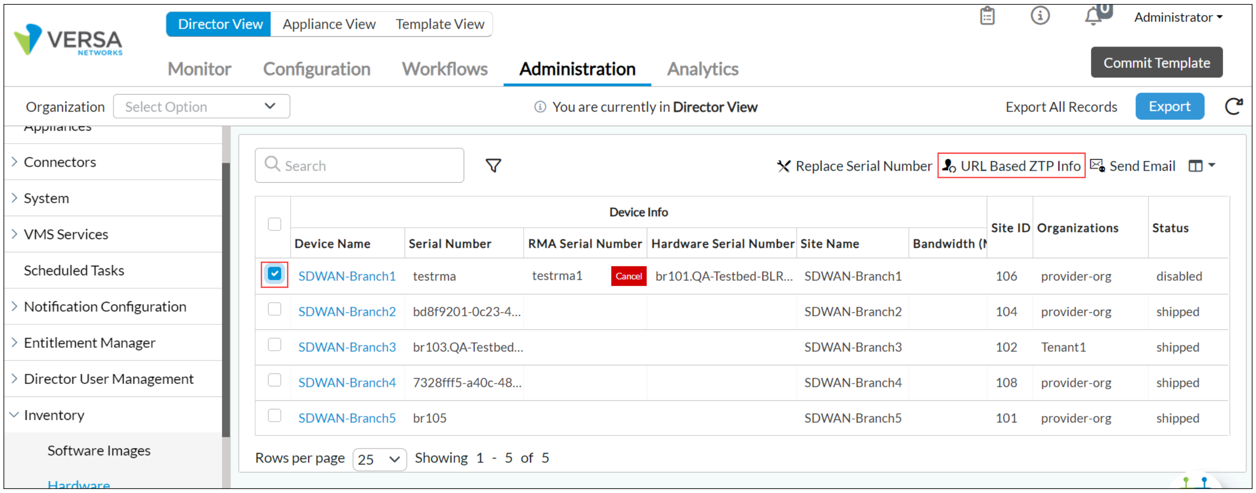
Rows per page 25 Showing 1 - 5 of 5

6. To use URL-based ZTP, load the default-device.cfg file.

```
admin@SDWAN-Branch1-cli(config)% load merge /opt/versa/etc/bootcfg/default-device.cfg
```

```
admin@SDWAN-Branch1-cli(config)% commit
```

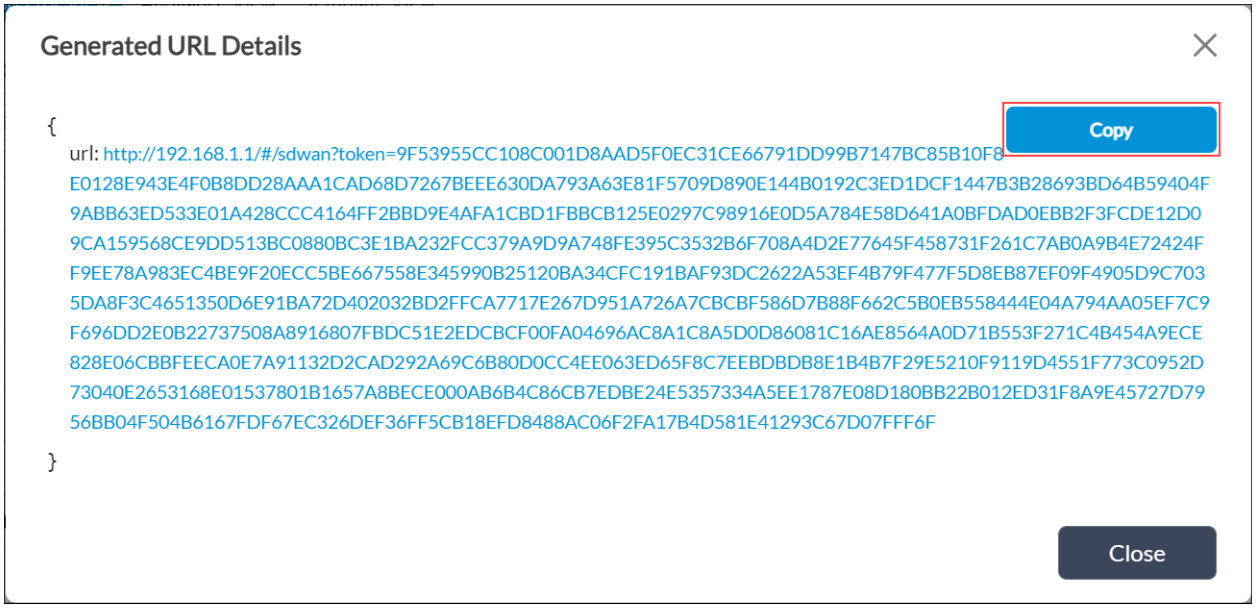
7. Select the device, and then click the URL Based ZTP Info icon.



| □ | Device Info | | | | | | Site ID | Organizations | Status |
|---|---|---|---|---|---|---|---|---|---|
| | Device Name | Serial Number | RMA Serial Number | Hardware Serial Number | Site Name | Bandwidth (I | | | |
| ☑ | SDWAN-Branch1 | testrma | testrma1 Cancel | br101.QA-Testbed-BLR... | SDWAN-Branch1 | | 106 | provider-org | disabled |
| □ | SDWAN-Branch2 | bd8f9201-0c23-4... | | | SDWAN-Branch2 | | 104 | provider-org | shipped |
| □ | SDWAN-Branch3 | br103.QA-Testbed... | | | SDWAN-Branch3 | | 102 | Tenant1 | shipped |
| □ | SDWAN-Branch4 | 7328fff5-a40c-48... | | | SDWAN-Branch4 | | 108 | provider-org | shipped |
| □ | SDWAN-Branch5 | br105 | | | SDWAN-Branch5 | | 101 | provider-org | shipped |

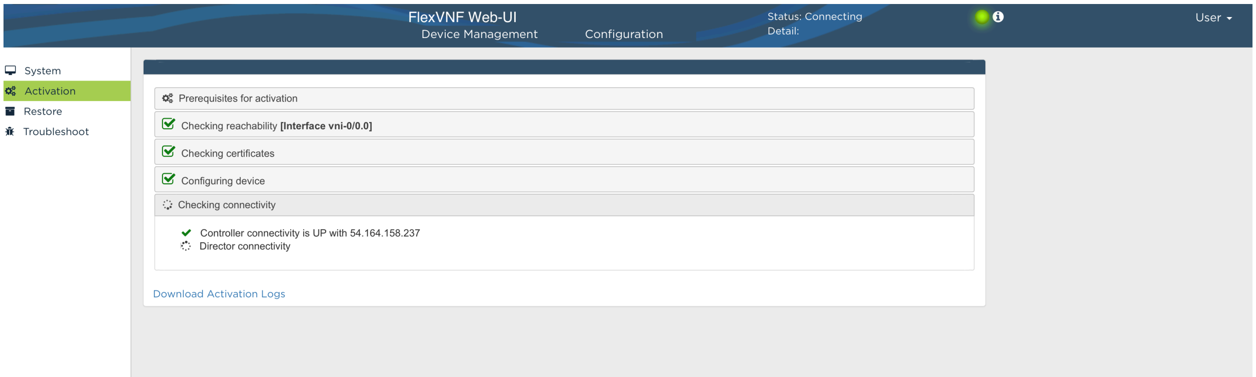
Rows per page 25 Showing 1 - 5 of 5

8. In the Generated URL Details popup window, click Copy to copy the URL.



```
{
  url: http://192.168.1.1/#/sdwan?token=9F53955CC108C001D8AAD5F0EC31CE66791DD99B7147BC85B10F8
  E0128E943E4F0B8DD28AAA1CAD68D7267BEEE630DA793A63E81F5709D890E144B0192C3ED1DCF1447B3B28693BD64B59404F
  9ABB63ED533E01A428CCC4164FF2BBD9E4AFA1CBD1FBBCB125E0297C98916E0D5A784E58D641A0BFDAD0EBB2F3FCDE12D0
  9CA159568CE9DD513BC0880BC3E1BA232FCC379A9D9A748FE395C3532B6F708A4D2E77645F458731F261C7AB0A9B4E72424F
  F9EE78A983EC4BE9F20ECC5BE667558E345990B25120BA34CFC191BAF93DC2622A53EF4B79F477F5D8EB87EF09F4905D9C703
  5DA8F3C4651350D6E91BA72D402032BD2FFCA7717E267D951A726A7CBCBF586D7B88F662C5B0EB558444E04A794AA05EF7C9
  F696DD2E0B22737508A8916807FBDC51E2EDCBCF00FA04696AC8A1C8A5D0D86081C16AE8564A0D71B553F271C4B454A9ECE
  828E06CBBFEECA0E7A91132D2CAD292A69C6B80D0CC4EE063ED65F8C7EEBDBDB8E1B4B7F29E5210F9119D4551F773C0952D
  73040E2653168E01537801B1657A8BECE000AB6B4C86CB7EDBE24E5357334A5EE1787E08D180BB22B012ED31F8A9E45727D79
  56BB04F504B6167FDF67EC326DEF36FF5CB18EFD8488AC06F2FA17B4D581E41293C67D07FFF6F
}
```

9. Paste the URL in any browser, and then change the IP address to device's IP address.
10. In the Device Management tab, click Start Activation to start the ZTP activation of the VOS device. For more information, see Activate VOS Devices.



Prerequisites for activation

✓ Checking reachability **[Interface vni-0/0.0]**

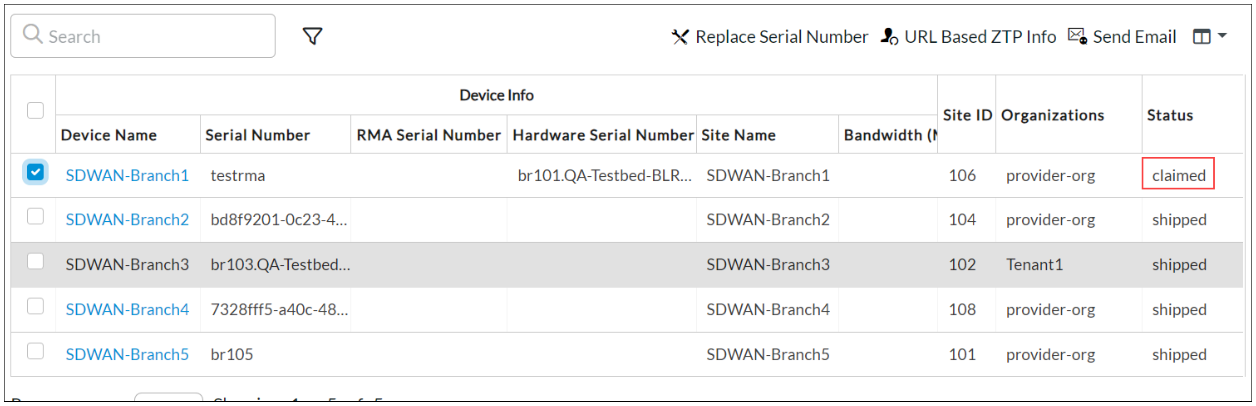
✓ Checking certificates

✓ Configuring device

Checking connectivity

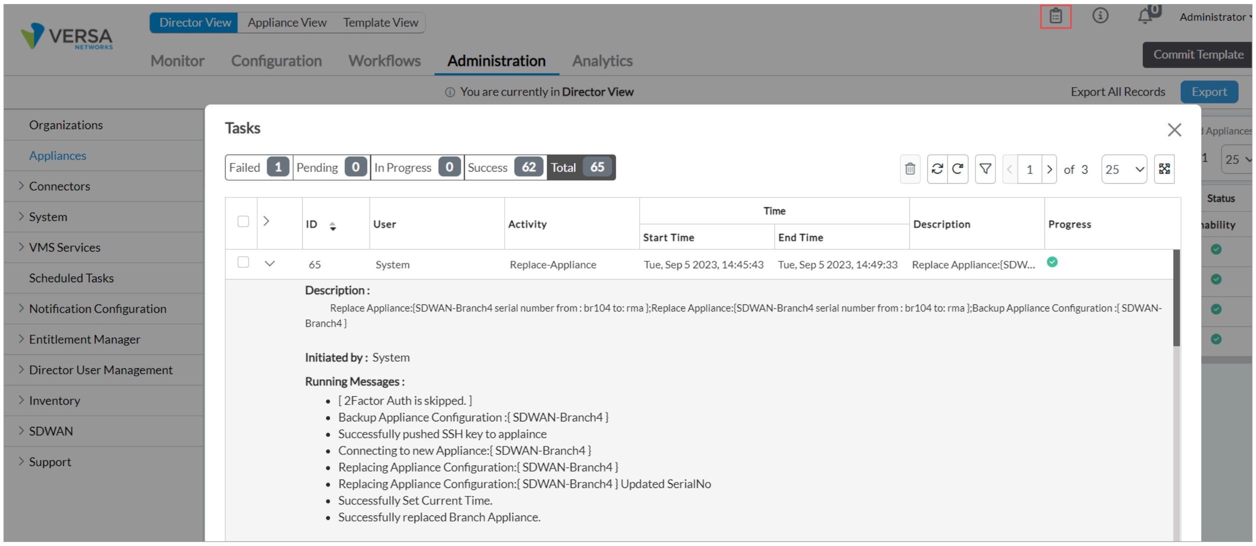
- ✓ Controller connectivity is UP with 54.164.158.237
- Director connectivity

11. After the RMA completes, the status of the device shows as Claimed.



| □ | Device Info | | | | | | Site ID | Organizations | Status |
|---|---|---|---|---|---|---|---|---|---|
| | Device Name | Serial Number | RMA Serial Number | Hardware Serial Number | Site Name | Bandwidth (M | | | |
| ☑ | SDWAN-Branch1 | testrma | | br101.QA-Testbed-BLR... | SDWAN-Branch1 | | 106 | provider-org | claimed |
| □ | SDWAN-Branch2 | bd8f9201-0c23-4... | | | SDWAN-Branch2 | | 104 | provider-org | shipped |
| □ | SDWAN-Branch3 | br103.QA-Testbed... | | | SDWAN-Branch3 | | 102 | Tenant1 | shipped |
| □ | SDWAN-Branch4 | 7328fff5-a40c-48... | | | SDWAN-Branch4 | | 108 | provider-org | shipped |
| □ | SDWAN-Branch5 | br105 | | | SDWAN-Branch5 | | 101 | provider-org | shipped |

12. To check the status of RMA process and to view any error messages, click the 📋 Tasks icon, and then check the task created for the replacement appliance.



| | ID | User | Activity | Time | | Description | Progress |
|---|---|---|---|---|---|---|---|
| | | | | Start Time | End Time | | |
| ☐ | 65 | System | Replace-Appliance | Tue, Sep 5 2023, 14:45:43 | Tue, Sep 5 2023, 14:49:33 | Replace Appliance:{SDW... | ✓ |

**Description :**
Replace Appliance:{SDWAN-Branch4 serial number from : br104 to: rma };Replace Appliance:{SDWAN-Branch4 serial number from : br104 to: rma };Backup Appliance Configuration :{ SDWAN-Branch4 }

**Initiated by :** System

**Running Messages :**

- [ 2Factor Auth is skipped. ]
- Backup Appliance Configuration :{ SDWAN-Branch4 }
- Successfully pushed SSH key to applaince
- Connecting to new Appliance:{ SDWAN-Branch4 }
- Replacing Appliance Configuration:{ SDWAN-Branch4 }
- Replacing Appliance Configuration:{ SDWAN-Branch4 } Updated SerialNo
- Successfully Set Current Time.
- Successfully replaced Branch Appliance.

13. If the device does not support URL ZTP, onboard the device using the normal ZTP process, which uses CLI commands. For more information, see Activate VOS Devices.

## Redeploy VMs and Cloud Devices after RMA

Typically, you redeploy a VM when the VM environment fails or when you upgrade from Ubuntu 14 (Trusty) to Ubuntu 18 (Bionic).

The procedure in this section applies to devices running Releases 21.2.3 or later regardless of whether password encryption is enabled. For devices on which password encryption is enabled, the individual encryption keys and the replacement device's key can decrypt the passwords in the device's configuration that is stored on the Director node. The procedure in this section also applies devices running earlier software releases on which password encryption is not enabled. If password encryption is enabled, follow the procedure in Redeploy VOS Devices Running Release 20.2 through Release 21.2.2 after RMA, below.

VMs and cloud devices can emulate a serial number, and branch devices that are VMs or cloud devices use this serial number to receive their configuration from the Director node. It is recommended that you use two-factor authentication for device staging to protect devices from being replicated.

To redeploy a VM or cloud device, you restage the device using script-based ZTP with the same serial number. For more information, see Activate VOS Devices.

## Redeploy VOS Devices Running Release 20.2 through Release 21.2.2 after RMA

For VOS devices running Release 20.2 through Release 21.2.2 and on which password encryption is enabled, the new device's encryption key cannot decrypt the passwords in the configuration stored on the Director node. Therefore, to redeploy the replacement hardware, you must delete the device configuration from the Director node and then use ZTP to onboard the replacement devices as if they were new devices. (For more information, see Activate VOS Devices.) This process uses the template and bind data stored in the Director configuration database and generates a new configuration for the replacement device.

If necessary, the Director node can replace the VOS software on the replacement device. The Director node fetches the required information from the replacement VOS device. If the device is unreachable, the Director node retries later. After the Director node fetches the information, you can redeploy the device.

Note that if you need to replace a hub-controller node (HCN), you must redeploy all spoke device workflows after the you onboard the HCN.

## Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- For Releases 21.2.3 and later, you can RMA devices on which encryption is enabled without deleting the device's configuration on the Director node.

## Additional Information

Activate VOS Devices
How To Return Hardware