Identify vEdge Certificate Expired on May 9, 2023

Contents

Introduction

This document describes how to identify a vEdge with an expired certificate that can affect control connections, and data plane connections, and result in loss of service.

Background Information

This issue impacts vEdge 100M, vEdge 100WM, vEdge 100B, vEdge 1000, and vEdge 2000 platforms. This is caused by a public root certificate that expired on May 9th, 2023 at 6:57 AM UTC.

> **Note**: This incident does not impact these platforms:
>
> 1. vEdge Cloud, vEdge 5000, and ISR 1100 running Viptela OS
>
> 2. Cisco routing platforms (physical as well as virtual) running XE SD-WAN software

---

<#root>

vEdge#

show control local-properties

```
personality                     vedge
sp-organization-name            CALO - 100589
organization-name               CALO - 100589
root-ca-chain-status            Installed
certificate-status              Installed
certificate-validity            Not Valid -  certificate has expired    <<<<<<<<<<<<<<<<<<<<
certificate-not-valid-before    May 12 17:11:21 2013 GMT
certificate-not-valid-after     Jan 19 03:14:07 2038 GMT
```

In case the device got reloaded after the 'hour X' (that is 6:57 AM UTC May 9th, 2023) additionally this is seen:

```
serial-num BOARD-ID-NOT-INITIALISED
```

> **Caution**: This issue is applicable when the Hardware WAN Edge Certificate Authorization is set to either Enterprise Certificates or Onbox Certificates in vManage.

These conditions can result in an impact on the vEdge:

1. Loss of connections to vSmart
2. Loss of connections to vManage
3. Port-Hop
4. Control policy changes such as topology changes in the network
5. Clear control connection
6. Interface Flaps

7. Device Reload

> **Note**: During the Control Connection establishment, the Onbox certificate is validated by the controllers in all cases. When Enterprise Certificates are used, both the Onbox and Enterprise Certificates are validated.

> **Note**: For more information about this behavior, reference Cisco bug ID CSCwf28118.

Precautions to Avoid Service Disruption

In order to prevent a complete loss of service, AVOID these actions in this section.

1. Reload the device
2. Update policy
3. Template pushes

> **Caution**: Device reload causes the Graceful Restart Timers to reset and the router is not able to reconnect to the fabric. Without a reload, the Data Plane (BFD) Sessions remain up and traffic is able to pass until the Graceful Restart timer is expired, even while control connections are down.

Remediation Process

Cisco has published upgrade versions of software to permanently resolve this problem. Carefully read the entire process before you take any action.

The high-level process to remedy this problem is:

1. Execute pre-checks to prepare for the upgrade of your Controller(s)
2. Upgrade the SD-WAN controller(s) to a fixed version
3. Restore control and BFD connections between vEdge and controllers
4. Execute pre-checks to prepare to upgrade your vEdge software
5. Upgrade vEdge software to a fixed version
6. Post-Upgrade Considerations

Three scenarios are referenced here. The steps for remediation vary based on which scenario applies to each vEdge in your network.

Scenario 1: vEdge Control Connection is UP and the vEdge HAS NOT been rebooted.

Scenario 2: vEdge Control Connection is DOWN and the vEdge HAS NOT been rebooted.

Scenario 3: vEdge Control Connection is DOWN and the vEdge HAS been rebooted.

Fixed Software Versions

Cisco continues to work to build and validate fixed software versions as quickly as possible. This page is updated as new versions are validated and posted to Cisco.com.

> **Tip**: Use the 'My Notifications' feature found on the Software Downloads page on Cisco.com to be

notified when new software is available for any Cisco product you are interested in.

Use the table shown to determine which version you can upgrade to based on your current version. It is possible more than one upgrade path is supported.

More versions are added as they are available. If your version is not listed in the **Current Version** column there is no upgrade path available at this time.

Tip: It is advisable to stage software images prior to the scheduled Maintenance Window. Use **Install** to stage the images prior to the window. Do not check the box **Activate and Reboot** during this process otherwise, the device completes the upgrade immediately after the completion of the install. This ensures a shorter Maintenance Window.

Note: In order to ensure the integrity of an image at Cisco, customers can pursue a common best practice to verify it with the SHA checksum provided for the image. Cisco offers a Bulk Hash file as a helpful tool for customers to re-verify downloaded images from the Cisco Software Downloads page. For more detailed information, visit https://www.cisco.com/c/en/us/about/trust-center/downloads.html.

Upgrade Recommendation Matrix

The software versions in the table shown are recommended based on the fix for the expired certificate issue. Upgrades outside of the scope of this issue must only be done with the instructions in the product documentation and the Release Notes for Cisco SD-WAN based on the version you upgrade to.

Note: Cisco strongly recommends that you stay within your current release train to mitigate the impact on production due to the certification expiry issue. For example, If you are currently on 20.3.2, upgrade to 20.3.7.1.

Upgrading vEdge 5000, vEdge Cloud, and ISR 1100 is not currently necessary as they are not impacted, by Cisco bug ID CSCwf28118.

Current Version	Upgrade Version	Download Links
All versions earlier than 18.4	20.3.7.1	Call TAC to open a Service Request.
18.4 19.x	20.3.7.1	Read Upgrade Procedure from 18.4, 19.x and 20.1

20.1.x		
20.3.x	20.3.7.1	Vedge Software https://software.cisco.com/download/home/286320990/type/286321106/release/20.3.7.1 SD-WAN Software Update https://software.cisco.com/download/home/286320995/type/286321394/release/20.3.7.1 Read this Special Advisory with regard to previous recommended versions.
20.4.1 20.4.1.1 20.4.1.2 20.4.2	20.4.2.3	Vedge Software https://software.cisco.com/download/home/286320990/type/286321106/release/20.4.2.3 SD-WAN Software Update https://software.cisco.com/download/home/286320995/type/286321394/release/20.4.2.3 Read this Special Advisory before you upgrade.
20.6.1.1	20.6.1.2	vEdge Software https://software.cisco.com/download/home/286320990/type/286321106/release/20.6.1.2 SD-WAN Software Update https://software.cisco.com/download/home/286320995/type/286321394/release/20.6.1.2
20.6.2 20.6.3.1	20.6.3.2	vEdge Software: https://software.cisco.com/download/home/286320990/type/286321106/release/20.6.3.2 SD-WAN Software Update: https://software.cisco.com/download/home/286320995/type/286321394/release/20.6.3.2 Read this Special Advisory before you upgrade.
20.6.4	20.6.4.1	vEdge Software https://software.cisco.com/download/home/286320990/type/286321106/release/20.6.4.1 SD-WAN Software Update https://software.cisco.com/download/home/286320995/type/286321394/release/20.6.4.1 Read this Special Advisory before you upgrade.

20.5.x 20.6.5	20.6.5.2	vEdge Software https://software.cisco.com/download/home/286320990/type/286321106/release/20.6.5.2 SD-WAN Software Update https://software.cisco.com/download/home/286320995/type/286321394/release/20.6.5.2
20.7.x 20.8.x 20.9.x	20.9.3.1	vEdge Software https://software.cisco.com/download/home/286320990/type/286321106/release/20.9.3.1 Read this note with regards to vEdge hardware compatibility with this release. SD-WAN Software Update https://software.cisco.com/download/home/286320995/type/286321394/release/20.9.3.1
20.10	20.10.1.1	SD-WAN Software Update https://software.cisco.com/download/home/286320995/type/286321394/release/20.10.1.1 Check the compatibility matrix to select the vEdge software version.
20.11.1	20.11.1.1	SD-WAN Software Update https://software.cisco.com/download/home/286320995/type/286321394/release/20.11.1.1 Check the compatibility matrix to select the vEdge software version.

Note: For mixed-version environments, perform software upgrades per the recommendations in the table shown based on the image the device is currently running.

Check the compatibility matrix to identify any possible controller/edge compatibility issues and open a TAC SR for support if any concerns arise.

Note: Customers on Engineering Special (ES) images who have not yet upgraded to an image with the fix need to open a TAC SR for further guidance.

---

vEdge-2000 Compatibility

The last supported software image train for vEdge-2000 is 20.9.x.

vEdge-100B, vEdge-100M, vEdge-1000 Compatibility

The last supported software image train for vEdge-100B, vEdge-100M, and vEdge-1000 is 20.6.x. Use the current version and the software image in the in order to identify the recommended target release.

If the vEdge-100B, vEdge-100M, and vEdge-1000 happen to already be on 20.7.x and later, open to a TAC SR for guidance.

> **Caution**: Due to the potential impact on production, we advise our customers to only execute the upgrades during a maintenance window. Ensure and confirm network stability prior to any additional changes to production.

SD-WAN Controller and vEdge Software Compatibility Matrix

> **Note**: Cisco strongly recommends that you stay within your current release train to mitigate the impact on production due to the certification expiry issue.
>
> For example, If you are currently on 20.3.2, upgrade to 20.3.7.1.
>
> Post upgrade for the certificate fix, if you choose to upgrade from one release train to another major release train, Cisco recommends you upgrade to the preferred release in that release train.
>
> For example, for post-certification fix: If you are currently on 20.3.7.1 and plan to upgrade to the 20.6 release train, Cisco recommends that you upgrade to the preferred version 20.6.5.2 release.

SD-WAN Controllers	vEdge 100M, vEdge 100B, vEdge 1000	vEdge 2000
20.3.3.2[1]	20.3.3.2[1]	20.3.3.2[1]
20.3.4.3[1]	20.3.3.2[1], 20.3.4.3[1]	20.3.3.2[1], 20.3.4.3[1]
20.3.5.1[1]	20.3.3.2[1], 20.3.4.3[1], 20.3.5.1[1]	20.3.3.2[1], 20.3.4.3[1], 20.3.5.1[1]
20.3.7.1[2]	20.3.3.2[1], 20.3.4.3[1], 20.3.5.1[1], **20.3.7.1[2]**	20.3.3.2[1], 20.3.4.3[1], 20.3.5.1[1], **20.3.7.1[2]**
20.4.2.3	20.3.3.2[1], **20.3.7.1[2]**, 20.4.2.3	20.3.3.2[1], **20.3.7.1[2]**, 20.4.2.3
20.6.1.2	20.6.1.2	20.6.1.2
20.6.3.2	20.3.3.2[1], 20.3.4.3[1], 20.3.5.1[1], **20.3.7.1[2]**, 20.4.2.3, 20.6.1.2,	20.3.3.2[1], 20.3.4.3[1], 20.3.5.1[1], **20.3.7.1[2]**, 20.4.2.3,

	20.6.3.2	20.6.1.2, 20.6.3.2
20.6.4.1	20.3.3.2[1], 20.3.4.3[1], 20.3.5.1[1], 20.4.2.3, 20.6.1.2, 20.6.3.2, 20.6.4.1	20.3.3.2[1], 20.3.4.3[1], 20.3.5.1[1], 20.4.2.3, 20.6.1.2, 20.6.3.2, 20.6.4.1
20.6.5.2[2]	20.3.3.2[1], 20.3.4.3[1], 20.3.5.1[1], **20.3.7.1[2]**, 20.4.2.3, 20.6.1.2, 20.6.3.2, 20.6.4.1, **20.6.5.2[2]**	20.3.3.2[1], 20.3.4.3[1], 20.3.5.1[1], **20.3.7.1[2]**, 20.4.2.3, 20.6.1.2, 20.6.3.2, 20.6.4.1, **20.6.5.2[2]**
20.9.3.1[2]	20.3.3.2[1], 20.3.4.3[1], 20.3.5.1[1], **20.3.7.1[2]**, 20.4.2.3, 20.6.1.2, 20.6.3.2, 20.6.4.1, **20.6.5.2[2]**	20.3.3.2[1], 20.3.4.3[1], 20.3.5.1[1], **20.3.7.1[2]**, 20.4.2.3, 20.6.1.2, 20.6.3.2, 20.6.4.1, **20.6.5.2[2]**, **20.9.3.1[2]**
20.10.1.1	20.6.1.2, 20.6.3.2, 20.6.4.1	20.6.1.2, 20.6.3.2, 20.6.4.1
20.11.1.1	20.6.1.2, 20.6.3.2, 20.6.4.1, **20.6.5.2[2]**	20.6.1.2, 20.6.3.2, 20.6.4.1, **20.6.5.2[2]**, **20.9.3.1[2]**

[1]This image is no longer available for download. They are documented for customers that have already deployed them.

[2]Indicates a **preferred** release that contains the certificate fix.

Pre-checks to Be Performed Prior to a Controller Upgrade

Backup your Controller

- If cloud-hosted, confirm the latest backup is done or initiate a backup of **config db** as mentioned in the next step.
  - You can view the current backups as well as trigger an on-demand snapshot from the SSP portal. Find more guidance here.
- If on-prem, take a **config-db** backup and VM snapshot of the controllers.

<#root>

vManage#

request nms configuration-db backup path /home/admin/db_backup

successfully saved the database to /home/admin/db_backup.tar.gz

- If on-prem, collect the **show running-config** and save this locally.
- If on-prem, ensure you know your **neo4j** password and notate to your exact current version.

Run an AURA Check

- Download and adhere to the steps in order to run AURA from CiscoDevNet/sure: SD-WAN Upgrade Readiness Experience
- Open to a TAC SR in order to address any questions related to the failed checks in the AURA report.

Ensure Send to Controllers/Send to vBond is Done

Check vManage Statistics Collection Interval

Cisco recommends the Statistics Collection Interval in **Administration > Settings** is set to the default timer of 30 minutes.

> **Note**: Cisco recommends that your vSmarts and vBonds be attached to the vManage template before an upgrade.

Verify Disk Space on vSmart and vBond

Use the command **df -kh | grep boot** from vShell to determine the size of the disk.

```
controller:~$ df -kh | grep boot
/dev/sda1       2.5G  232M  2.3G  10% /boot
controller:~$
```

If the size is greater than 200 MB, proceed with the upgrade of the controllers.

If the size is less than 200 MB, pursue these steps:

1. Verify the current version is the only one listed under **show software** command.

```
VERSION    ACTIVE   DEFAULT PREVIOUS  CONFIRMED TIMESTAMP
--------------------------------------------------------------------------------
20.11.1     true    true    false    auto     2023-05-02T16:48:45-00:00
20.9.1      false   false   true     user     2023-05-02T19:16:09-00:00
20.8.1      false   false   false    user     2023-05-10T10:57:31-00:00
```

2. Verify the current version is set as default under **show software version** command.

```
controller# request software set-default 20.11.1
status mkdefault 20.11.1: successful
controller#
```

3. If more versions are listed, remove any versions not active with the command **request software remove <version>**. This increases the space available to proceed with the upgrade.

```
controller# request software remove 20.9.1
status remove 20.9.1: successful
vedge-1# show software
VERSION   ACTIVE DEFAULT PREVIOUS CONFIRMED TIMESTAMP
-------------------------------------------------------------------------------
20.11.1   true   true    false    auto      2023-05-02T16:48:45-00:00
controller#
```

4. Check the disk space in order to ensure it is greater than 200 MB. If it is not, open a TAC SR.

Upgrade your Controllers

This is a summary of the next steps which are done for each of these customers.

Caution: Confirm all prechecks are done and backups taken as described in the previous section.

- Upload the new software version to the upgrade repository.
- Ensure the controller image with the fix for this problem is selected.
- Upgrade the controllers with the image fix in this sequence.
  1. vManage
  2. vBond
  3. vSmart

Note: If you proceed with the controllers upgrade by CLI, remember to perform '**request software upgrade-confirm**'.

---

vManage Standalone Upgrade

In the case of standalone vManage, these steps must be pursued:

1. Copy the image to vManage **Maintenance> Software repository**
2. Upgrade with vManage **Maintenance>Software upgrade**
3. Click **Upgrade**, and wait for the upgrade to complete
4. Navigate back to the same page, click the vManage, and then click **Activate**

Note: The vManage upgrade has no impact on the data network.

---

vManage Cluster Upgrade

In the case of cluster upgrade, the steps mentioned in the Cisco SD-WAN Getting Started Guide - Cluster Management [Cisco SD-WAN] - Cisco guide must be pursued.

Note: The vManage cluster upgrade has no impact on the data network.

Caution: If you have any questions or issues when you upgrade your cluster, contact TAC before you proceed.

vBond Upgrade

A vBond upgrade uses the same process as a vManage upgrade.

Warning: vBonds must be upgraded sequentially. Verify the upgrade has been completed on each vBond before you move to the next.

1. Copy the image to **vManage Maintenance > Software repository**
2. Upgrade with **vManage Maintenance > Software upgrade**
3. Click **Upgrade**, and wait for the upgrade to complete
4. Navigate back to the same page, click vManage, and then click **Activate**
5. Verify with the command **show orchestrator connections** on the vBond
6. Verify with the command **show control connections** on the vManage

vSmart Upgrade

A vSmart upgrade uses the same process as a vManage upgrade.

Warning: vSmarts must be upgraded sequentially. Verify the upgrade has been completed on each vSmart before you move to the next.

1. Copy the image to **vManage Maintenance > Software repository**
2. Upgrade the vSmart from the **vManage UI Maintenance > Software upgrade**
3. Click **Upgrade** and wait for the upgrade to complete
4. Navigate back to the same page. Choose the vSmart then click **Activate**
5. Verify sessions have been restored after the upgrade with the command **show control connections** on the vSmart

Note: When the vSmart reboots during a software upgrade, devices run into graceful restart with no network impact.

Verify Control Connections are Established After all Controller Upgrades

For all vEdge in **Scenario 1** and **Scenario 2** after the Controller(s) have been upgraded both Control and BFD connections must be restored.

Upgrade vEdge

Note: vEdge upgrade is the last step of the procedure to completely protect against the power cycle of the vEdge routers, described in **Scenario 3**.

Note: It is advisable to stage vEdge software images prior to the scheduled Maintenance Window. Use **Install** to stage the images prior to the window. Do not check the box **Activate and Reboot** during this process otherwise, the device completes the upgrade immediately after the completion of the install. This ensures a shorter Maintenance Window.

You can load the images to multiple vEdges at one go from vManage via:

1. Navigate to the vManage UI. Navigate to **Maintenance > Software Repository**. Load the vEdge image. You can then navigate to **Maintenance > Software Upgrade** and click **Upgrade** after you choose the devices that need the upgrade.

2. Navigate to the vManage UI. Navigate to **Maintenance > Software Repository**. Click **Add new software**. Click **Remote server**. Enter the controller version, the vEdge version, and the complete path to the **FTP/HTTP** URL where the image is stored. For example, **ftp://<username>:<password>@<FTP server>/<path>/<image name>**. You can then navigate to **Maintenance > Software Upgrade** and click **Upgrade** after you choose the devices that need the upgrade with the use of the **Remote server** option.

Note: Choose vEdges in batches based on the bandwidth in order to push the image.

Prechecks Before vEdge Upgrade

Caution: If these prechecks are skipped, the vEdge upgrade can fail due to insufficient disk space.

1. Verify the current version is the only one listed under **show software** command.

```
VERSION    ACTIVE   DEFAULT PREVIOUS  CONFIRMED TIMESTAMP
-------------------------------------------------------------------------------
20.11.1     true    true    false    auto     2023-05-02T16:48:45-00:00
20.9.1      false   false   true     user     2023-05-02T19:16:09-00:00
20.8.1      false   false   false    user     2023-05-10T10:57:31-00:00
```

2. Verify the current version is set as default under **show software version** command.

```
vedge-1# request software set-default 20.11.1
status mkdefault 20.11.1: successful
vedge-1#
```

3. If more versions are listed, remove any versions not active with the command **request software remove <version>**. This increases the space available to proceed with the upgrade.

```
vedge-1# request software remove 20.9.1
status remove 20.9.1: successful
vedge-1# show software
VERSION   ACTIVE DEFAULT PREVIOUS CONFIRMED TIMESTAMP
-------------------------------------------------------------------------------
20.11.1   true   true    false    auto      2023-05-02T16:48:45-00:00
vedge-1#
```

4. Use **vShell** and command **df -h** in order to confirm there is enough free disk space to perform the upgrade.

```
VEDGE-1000-AC-K9# vshel
VEDGE-1000-AC-K9:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
none            1.4G  8.0K  1.4G   1% /dev
/dev/sda1      1013M  518M  445M  54% /boot
/dev/loop0       78M   78M     0 100% /rootfs.ro
/dev/sda2       6.0G  178M  5.5G   4% /rootfs.rw
aufs            6.0G  178M  5.5G   4% /
tmpfs           1.4G  300K  1.4G   1% /run
shm             1.4G   48K  1.4G   1% /dev/shm
tmp             600M   84K  600M   1% /tmp
tmplog          120M   37M   84M  31% /var/volatile/log/tmplog
svtmp           1.0M  312K  712K  31% /etc/sv
```

5. If /tmp is full, open a TAC SR to get assistance to clear space in the /tmp/tmp directory prior to the upgrade.

vEdge Upgrade Scenario 1: Control Connection is UP and vEdge HAS NOT Been Rebooted

After controllers are upgraded to a version with the fix, vEdge devices that have not been rebooted re-establish connectivity automatically.

> **Important**: An upgrade is required on vEdge devices in this state. It MUST be prioritized and planned as soon as possible. If needed, perform during off-business hours as quickly as possible. Plan an upgrade of the device in order to avoid control and data plane impact due to any reboot or power cycle of the device. The device must not be rebooted prior to the upgrade.

In order to upgrade the vEdge, pursue the steps indicated:

1. Copy the new vEdge software to the vManage via **Maintenance > Software repository**
2. Upgrade the vEdge from the **vManage Maintenance > Software upgrade**
3. Click**Upgrade**and wait for the upgrade to complete
4. Navigate back to the same page. Choose the vEdge and then click**Activate**

Post-Upgrade Validation

- Verify the control connections and BFD sessions

- Verify OMP routes and Service VPN routes - test end-to-end ping on every Service VPN segment between vEdge and Hub/other nodes
- Check the Post-Upgrade Considerations

vEdge Upgrade Scenario 2: Control Connection is Down and vEdge HAS NOT Rebooted

After controllers are upgraded to a version with the fix, vEdge devices that have not been rebooted re-establish connectivity automatically.

> **Important**: An upgrade is required on vEdge devices in this state. It MUST be prioritized and planned as soon as possible. If needed, perform during off-business hours as quickly as possible. Plan an upgrade of the device in order to avoid control and data plane impact due to any reboot or power cycle of the device. The device must not be rebooted prior to the upgrade.

In order to upgrade the vEdge, pursue the steps indicated:

1. Copy the new vEdge software to the vManage via **Maintenance > Software repository**
2. Upgrade the vEdge from the **vManage Maintenance > Software upgrade**
3. Click**Upgrade**and wait for the upgrade to complete
4. Navigate back to the same page. Choose the vEdge and then click**Activate**

Post-Upgrade Validation

- Verify the control connections and BFD sessions
- Verify OMP routes and Service VPN routes - test end-to-end ping on every Service VPN segment between vEdge and Hub/other nodes
- Check the Post-Upgrade Considerations

Scenario 3: vEdge, Control Connection is Down, the Device Rebooted/Power Cycled

---

> **Caution**: To recover these devices, out-of-band access is required.

This output shows a vEdge device that has been rebooted after the certificate expired. Use the command **show control local-properties | inc serial** and confirm the output shows BOARD-ID-NOT-INITIALISED.

```
vedge# show control local-properties | inc serial
serial-num                      BOARD-ID-NOT-INITIALISED
subject-serial-num              N/A
enterprise-serial-num           No certificate installed
vedge#
```

Change the Date/Time on vEdge to restore Control Connections

These steps require out-of-band access to the vEdge device such as console or direct SSH.

Roll back the clock to May 5th, 2023 (for example #**clock set date 2023-05-05 time 15:49:00.000**) on

vEdge which has a control connection DOWN.

```
vedge# clock set date 2023-05-05 time 10:23:00
vedge# show clock
Mon May 5 10:23:37 UTC 2023
vedge#
```

Wait 2-3 minutes for the board-id to initialize. Check **show control local-properties** in order to ensure the device now has a number shown in the output.

```
vedge# show control local-properties | inc serial
serial-num                      10024640
subject-serial-num              N/A
enterprise-serial-num           No certificate installed
vedge#
```

(Optional) If the board-id initialization does not happen within 2-3 minutes, reload vEdge and check the **show control local-properties** output in order to ensure the device now has its serial number listed in the output

Once the board-id has initialized validate the certificate with the command **show certificate validity**

```
vedge# show certificate validity
The certificate issued by c33d2cf4-e586-4df4-ac72-298422644ba3 is valid from Sep 7 02:50:16 2021 GMT (Cu
vedge#
```

Once control connections have been successfully recovered, correct the clock to the current time with a YYYY-MM-DD and HH:MM::SS format for the date and time.

This example is for illustration purposes only. Always set the date and time to the current time.

```
vedge# clock set date YYYY-MM-DD time HH:MM::SS
vedge# show clock
Wed May 10 10:23:37 UTC 2023
vedge#
```

Verify control connections are up with the command **show control connections**.

```
vedge# show control connections
                                                                                    PEER
PEER    PEER PEER            SITE       DOMAIN PEER                                 PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                           PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------------
```

```
vsmart  dtls 10.3.3.1       10         1      192.168.24.112                      12346 192.168.24.1
vsmart  dtls 10.3.3.1       10         1      192.168.24.112                      12346 192.168.24.1
vbond   dtls 0.0.0.0         0         0      192.168.28.122                      12346 192.168.28.1
vbond   dtls 0.0.0.0         0         0      192.168.28.122                      12346 192.168.28.1
vmanage dtls 10.1.1.1       10         0      192.168.25.209                      12346 192.168.25.2
```

> **Note**: An upgrade is required on vEdge devices in this state. It MUST be prioritized and planned as soon as possible. If needed, perform during a Maintenance Window during off-business hours. Plan an upgrade of the device to avoid impact due to any reboot or power cycle of the device. The device must not be rebooted prior to the upgrade.

In order to upgrade the vEdge, use these steps:

1. Copy the vEdge image fix to the vManage via **Maintenance > Software repository**
2. Upgrade the vEdge from the **vManage UI Maintenance > Software upgrade**
3. Click **Upgrade** and wait for the upgrade to complete
4. Navigate back to the same page. Choose the vEdge and then click **Activate**
   â€¢ Verify the control connections and BFD sessions are UP
   â€¢ Verify OMP routes and Service VPN routes - test end-to-end ping on every Service VPN segment between vEdge and Hub/other nodes
5. Check the Post-Upgrade Considerations

Upgrade Procedure from 18.4, 19.x, and 20.1 (Revised 13 May, 0300 UTC)

All upgrades from versions 18.4, 19.x, and 20.1.x must upgrade to version 20.3.7.1.

This section has been revised with instructions to upgrade vManage with boot disks smaller than 2.5G to 20.1.3.1 instead of 20.1.3.

The new 20.1.3.1 vManage software includes the updated certificates and allows devices to connect while the second upgrade to 20.3.7.1 is performed.

> **Caution**: Read this section carefully before you proceed. Multiple upgrades can be required.

Pre-Upgrade Checks

Before you proceed with any upgrade, you must complete all of the pre-checks to help ensure the upgrade is successful.

These pre-upgrade checks validate the size of the database, compute resources, and boot disk size.

Check Database Size via the CLI

Use the command request **nms configuration-db diagnostic | i TotalStoreSize** to obtain the size of the database in bytes.

From **vshell** execute the command **expr <number of bytes> / 1024 / 1024 / 1024** to convert this output to an integer value in GB.

```
vmanage# request nms configuration-db diagnostics | i TotalStoreSize
| "StoreSizes"     | "TotalStoreSize"                    | 3488298345                |
vmanage1# vshell
vmanage1:~$ expr 348829834 / 1024 / 1024 / 1024
3
```

This example shows the database size is 3 GB.

> **STOP**: If your database size is 5GB or greater **Open a TAC SR** for assistance with this upgrade.

If the database size is less than 5GB proceed with the upgrade.

Verify Compute Resources

Ensure Compute resources are in line with the 20.3 Compute Resources Guide.

- Check vCPU with the command **lscpu | grep CPU\ MHz**

```
vmanage1:~$ lscpu | grep CPU\ MHz
CPU MHz:                 2999.658
vmanage1:~$
```

- Check Memory with the commands **free -g | grep Mem** and **free --giga | grep Mem**

```
vmanage1:~$ free -g | grep Mem
Mem:          31          21           7           0           2           9
vmanage1:~$ free --giga | grep Mem
Mem:          33          23           7           0           2           9
vmanage1:~$
```

- Check Third Partition (**/opt/data**) size with the command **df -kh**

<#root>

```
vmanage1:~$ df -kh | grep "/opt/data"
/dev/sdb        108G   24G   79G  23% /opt/data
vmanage1:~$
```

If compute resources are not in line with 20.3, increase the computing resources prior to the upgrade.

Check Boot Disk Space with CLI

Use the command **df -kh | grep boot** from vShell in order to determine the size of the disk.

```
vmanage# vshell
vmanage:~$ df -kh | grep boot
/dev/sda1       5.0G  4.7G  343M  94% /boot
vmanage:~$
```

This example shows the **/boot disk** is 5.0G.

> **Warning**: If the vManage boot disk is less than 2.5G you must perform a step upgrade through version 20.1

Upgrade vManage on Versions 18.4 and 19.x

Perform the Upgrade - vManage Standalone

If the size of the boot disk is **less than 2.5G** you must upgrade vManage to version 20.1 before you proceed.

- Download the 20.1.3.1 image from https://software.cisco.com/download/home/286320995/type/286321394/release/20.1.3.1
- Pursue the steps in Upgrade your Controllers to complete the upgrade

If the disk size is **2.5G or greater** you can upgrade to 20.3.7.1 directly.

- Download the 20.3.7.1 image from https://software.cisco.com/download/home/286320995/type/286321394/release/20.3.7.1
- Pursue the steps in Upgrade your Controllers to complete the upgrade

Perform the Upgrade - vManage Cluster

If the size of the disk is **less than 2.5G** you must upgrade vManage to version 20.1.3.1 before you proceed.

> **STOP**: Open a TAC SR for assistance to step upgrade on the vManage cluster.

If the disk size is **2.5G or greater** you can upgrade to 20.3.7.1 directly.

- Download the 20.3.7.1 image from https://software.cisco.com/download/home/286320995/type/286321394/release/20.3.7.1
- Pursue the steps in Upgrade your Controllers to complete the upgrade

Upgrade vManage 20.1.x

Perform the Upgrade - vManage Standalone or Cluster

- Download the 20.3.7.1 image from https://software.cisco.com/download/home/286320995/type/286321394/release/20.3.7.1

- Pursue the steps in Upgrade your Controllers to complete the upgrade

Upgrade vSmart and vBond from 18.4, 19.x, or 20.1 to 20.3.7.1

vSmarts and vBonds can be upgraded directly from all versions to 20.3.7.1.

- Download the 20.3.7.1 image from https://software.cisco.com/download/home/286320995/type/286321394/release/20.3.7.1
- Pursue the steps in the Upgrade vSmart section to complete the upgrade
- Pursue the steps in the Upgrade vBond section to complete the upgrade

Upgrade vEdge from 18.4, 19.x, or 20.1 to 20.3.7.1

vSmarts, vBonds, and vEdge devices can be upgraded directly from all versions to 20.3.7.1.

- Download the 20.3.7.1 image from https://software.cisco.com/download/home/286320990/type/286321106/release/20.3.7.1
- Pursue the steps in the Upgrade vEdge section to complete the upgrade

Post-Upgrade Considerations

If configuration changes were made to increase graceful restart timers and IPSec rekey timers prior to the upgrade, it is recommended to roll the configurations back to the settings which were in place prior to the upgrade in order to avoid potential unnecessary impact.

Special Advisory

Customers who have upgraded their controllers to versions earlier than 20.3.7.1 and are in the process to upgrade their vEdges can reach out to TAC for access to respective vEdge images.

Advisory Regarding Cisco bug ID CSCwd46600

Previous versions of this document recommended customers upgrade to several versions of 20.3.x (20.3.3.2, 20.3.5.1, 20.3.4.3, 20.3.7.1).

Cisco recommends that customers who run image 20.3.x, upgrade their controllers and vEdges to image 20.3.7.1.

Devices that run releases 19.x and 20.3.x earlier than 20.3.7.1, 20.4, and 20.6x release earlier than 20.6.5.1 can encounter Cisco bug ID CSCwd46600 post-upgrade. In order to temporarily resolve this issue, run either of these commands:

<#root>

```
request security ipsec-rekey
```

or

<#root>

```
request port-hop color <color>
```

However, it is strongly recommended that the customers upgrade their controllers and vEdge devices to 20.3.7.1 or 20.6.5.1.

Customers that have completely upgraded all vEdge devices to a 20.3.x release prior to 20.3.7.1, 20.3.4.3, or a 20.6.x release prior to 20.6.5.1 based on previous guidance can choose to remain on this release if they have not been impacted by the bug. It is recommended to upgrade to 20.3.7.1 or 20.6.5.1 during a scheduled maintenance window at a later date.

Advisory for 20.6.x Release Train (Revised 15 May, 0800 UTC)

Previous versions of this document recommended customers upgrade to several versions of 20.6.x (20.6.3.2, 20.6.4.1, 20.6.5.2).

Cisco recommends that customers who run image 20.6.x and have trackers configured on an interface upgrade their controllers and vEdges to image 20.6.5.2.

Devices with a tracker configured can encounter Cisco bug ID CSCvz44093 during the upgrade. In order to avoid the impact of this bug you can remove the tracker configuration prior to the upgrade.

It is strongly recommended that customers upgrade their controllers and vEdge devices to 20.6.5.2.

Customers that have completely upgraded all vEdge devices to 20.6.3.2 and 20.6.4.1 based on previous guidance can choose to remain on this release if they have not been impacted by the bug.