OpenVPN server: Identifying / verifying certificate files on the Wave and OpenVPN server.

Last Modified on 01/05/2023 12:39 pm EST

Products Affected:

OpenVPN server: Vertical provided (CentOS6 or CentOS7 based) or customer provided & the Vertical Wave.

Purpose:

This article will help you identify where these certificates are stored and assist with verifying that they match what the OpenVPN server is expecting.

WARNING: Clicking options in the 'Certificate Maintenance' tab without checking the proper certificates exist may cause all deployed OpenVPN phones to become inoperable without manual intervention.

IMPORTANT: This article does NOT provide adequate information to cover migrating / changing OpenVPN servers with regards to certificates. To maintain continuity for existing VPN phones, ensure you have the 4 files in the bullet below from the OpenVPN server before proceeding further. Failure to do so will likely cause multiple OpenVPN connected phones needing manual intervention on their local network to restore connectivity.

- ca.crt, server.crt, server.key, & dh1024.pem

If you have any questions about anything in this article or concerns about migrating an OpenVPN server, please contact Vertical Technical Support for assistance before proceeding.

Client certificate:

The client certificate, VPNCertificate.crt, is present in all versions of Wave that support the OpenVPN server, i.e. 4.0 and above, and is located in the following folder:

- c:\inetpub\tftproot (this is used for all Edge IP 5000i gigabit phones)
- c:\inetpub\wwwroot\VIP (this is present only in Wave 5.0 and higher and is used for all Edge IP 9800 series phones supporting OpenVPN)

These files are currently part of a system backup (iobackup.cab).

Server certificate files:

Customer provided OpenVPN server:

You must work with the customer contact to verify that the client certificates match what they are expecting.

Vertical provided OpenVPN server:

- CentOS 6: the 4 files needed are located here: /etc/openvpn/easy-rsa/2.0/keys/

- CentOS 7: the 4 files needed are located here: /etc/openvpn/easy-rsa/3.0.8/keys

Wave:

When using the "Off-Wave" OpenVPN configurations (versions 4.5 and later), the Wave generates these keys and then pushes them to the OpenVPN server (Vertical provided OpenVPN server required).

IMPORTANT: The Wave has the master copies in this configuration and choosing to 'Re-deploy Certificate' will cause these files to overwrite both the OpenVPN server's copies as well as the client certificate file(s) listed earlier. If these files are NOT already present on the Wave, then the Wave WILL create new ones and potentially overwrite working certificates.

The same 4 files located on the OpenVPN server are located on the Wave here: C:\Program Files\easy-rsa\keys.

NOTE: There is a known issue where any of the following will cause the loss of the above listed directory:

- Wave Migration to later version (for versions 5.0 and later)
- IODD / restore to correct an issue.
- SSD replacement / restore due to HW failure.
    - This would not include a LiveImage restore.

However, even if this folder no longer exists on the Wave, it's absolutely likely that your current configuration will continue working.

Verifying certificates:

In Windows (on the Wave), it's trivial to verify these certificates match.

First open the client certificate by double clicking on it and choose the 'Details' tab. Here you can review the 'Serial number' as below.

Next, open the matching server side file on the Wave, this will be the ca.crt file, if it exists. If the 'Serial number' there matches, then you have a valid copy on the Wave. If the file does NOT exist, then...

1. Ensure you do NOT click the 'Re-deploy Certificate' button or you will likely render remote VPN phones inoperable.
2. You will need to review the OpenVPN server's copy to ensure you have a good working set.

In CentOS (6 or 7), reviewing the OpenVPN server's certificate will require a command.

While you can do this via the console to the OpenVPN server, it's recommended to simply use PuTTY and connect to the OpenVPN server from the Wave using the default port, 22.

Once logged in, first, determine the version of CentOS you're using with the following command:

```
cat /etc/centos-release
```

Then, use cd to change to the appropriate directory, as listed under the 'Vertical provided OpenVPN server' above, where the keys are stored. e.g. CentOS 7, type cd /etc/openvpn/easy-rsa/3.0.8/keys and press enter.

Once there, type the following to determine the serial number for your certificate:

```
openssl x509 -in ca.crt -serial -noout
```

example output:

```
[openvpn@openvpn keys]$ openssl x509 -in ca.crt -serial -noout
serial=A54111C2886781EC
```

NOTE: In Windows, the serial number shows a leading 00, you can disregard this when comparing to the CentOS output.

The certificates can be backed up from the OpenVPN server by using either psftp or WinSCP from the Wave.