Clearing FileWave Client Certs

In some situations, you may want to explicitly make the server clear and revoke a client certificate without deleting the client from FileWave, for instance if you are wiping a macOS client or reinstalling an IVS client.

From FileWave Central

For desktop clients, you can right-click the client and choose "Clear Certificate(s)".

Note that the current administrator needs to have write permissions on the clients, and will need to enter credentials.

From the Client

The first way is to use the client (13.1.1) certificate itself to authenticate, which is only possible if the certificate and its private key still exist on the client:

```
fwcld -clearCertificate [-serverHost <fwserver_address> -serverPort 20445]
```

This is the equivalent of the following command using curl (replace <fwserver_address> with the address of your FileWave server):

```
sudo curl --key /private/var/FileWave/client.key --cert /private/var/FileWave/client.crt -X POST
https://<fwserver_adress>:20445/auth/client/clear_certificate
```

The client will then be unable to communicate with the server (until a new CSR is created). This command can be used in the activation script of a macOS reinstall fileset to make the server properly clear the old client certificate.

Note that the command above uses the client certificate itself to identify the client. In case the certificate's private key is already lost, there is an alternative where you can authenticate with an administrator's token rather than with the client certificate:

```
fwcld -clearCertificate -token <application_token> [-serverHost <fwserver_address> -serverPort <fwserver_port>]
```

- <fwserver_address>: The FileWave server address (optional)
- <fwserver_port> : 20445 by default
- <application_token>: An administrator application token, with write permissions on this client. Can be found in the Application Tokens tab of the Manage Administrators dialog (example: {1ca3fe82-a41d-8866-bd4d-f83f9f1a8dd5}).

Alternatively, you can also clear certificates en masse using the inventory superadmin token. In this case, you are allowed to clear the certificate of any client (obviously use with caution):

```
curl -X POST https://<fwserver_address>:20445/auth/client/clear_certificates -H 'Authorization:
<application_token>' -H 'Content-Type: application/json' -d '["<serial_1>", "<serial_2>", ...]'
```

Included in 13.1.1 and above are the options to clear with 'MAC address' or 'Device ID':

```
curl -X POST https://<fwserver_address>:20445/auth/client/clear_certificates?identifier=mac -H 'Authorization:
<application_token_base64>' -H 'Content-Type: application/json' -d '["<mac_address_1>", "<mac_address_2>", ...]'
```

```
curl -X POST https://<fwserver_address>:20445/auth/client/clear_certificates?identifier=device_id -H
'Authorization: <application_token_base64>' -H 'Content-Type: application/json' -d '["<device_id_1>", "
<device_id_2>", ...]'
```

The identifier parameter is optional, its default value is serial_number.

- <fwserver_address>: The FileWave server address.
- <serial_1>, ...: serial numbers of clients to revoke. Must match the serial_number field from inventory.
- <mac_address_1>, ...: MAC addresses or clients to revoke.
- <device_id_1>, ...: device ids of clients to revoke.
- <application_token_base64>: base64-encoded value of an administrator application token, with write permission on this client. Can be found in the Application Tokens tab of the Manage Administrators dialog (example: ezFjYTNmZTgyLWE0MWQtODg2Ni1iZDRkLWY4M2Y5ZjFhOGRkNX0=_).

A dict of lists of clients for: SUCCESS, NOT_FOUND and ERROR statuses is returned.

- SUCCESS: the client certificate was successfully revoked.
- NOT_FOUND: no certificate was found on the server for this client, or no such client was found. Maybe the certificate was

already revoked, or the client had no certificate yet, or the client had not reported its MAC address or serial number yet, if you passed a MAC address or a serial number.
- ERROR: an unexpected error occurred. Please check server logs for details.

Potential log entries

```
2019-06-12 7:12:02.481|main|FATAL|CLIENT|Unable to retrieve the contents of the cached custom field values: Error decrypting data
2019-06-12 7:12:02.833|main|INFO|CLIENT|CRL updated
2019-06-12 7:12:02.834|main|INFO|CLIENT|No certificate private key yet. Sending a certificate signing request to server my.FQDN.com.
2019-06-12 7:12:03.235|main|FATAL|CLIENT|Failed to send enrollment request (and CSR): error 400 a CSR for this client was already sent.
2019-06-12 7:12:03.235|main|INFO|CLIENT|Falling back to no certificate.
```

Revision #2
★Created 14 July 2023 19:03:15 by Josh Levitsky
Updated 19 September 2024 17:11:06 by Josh Levitsky