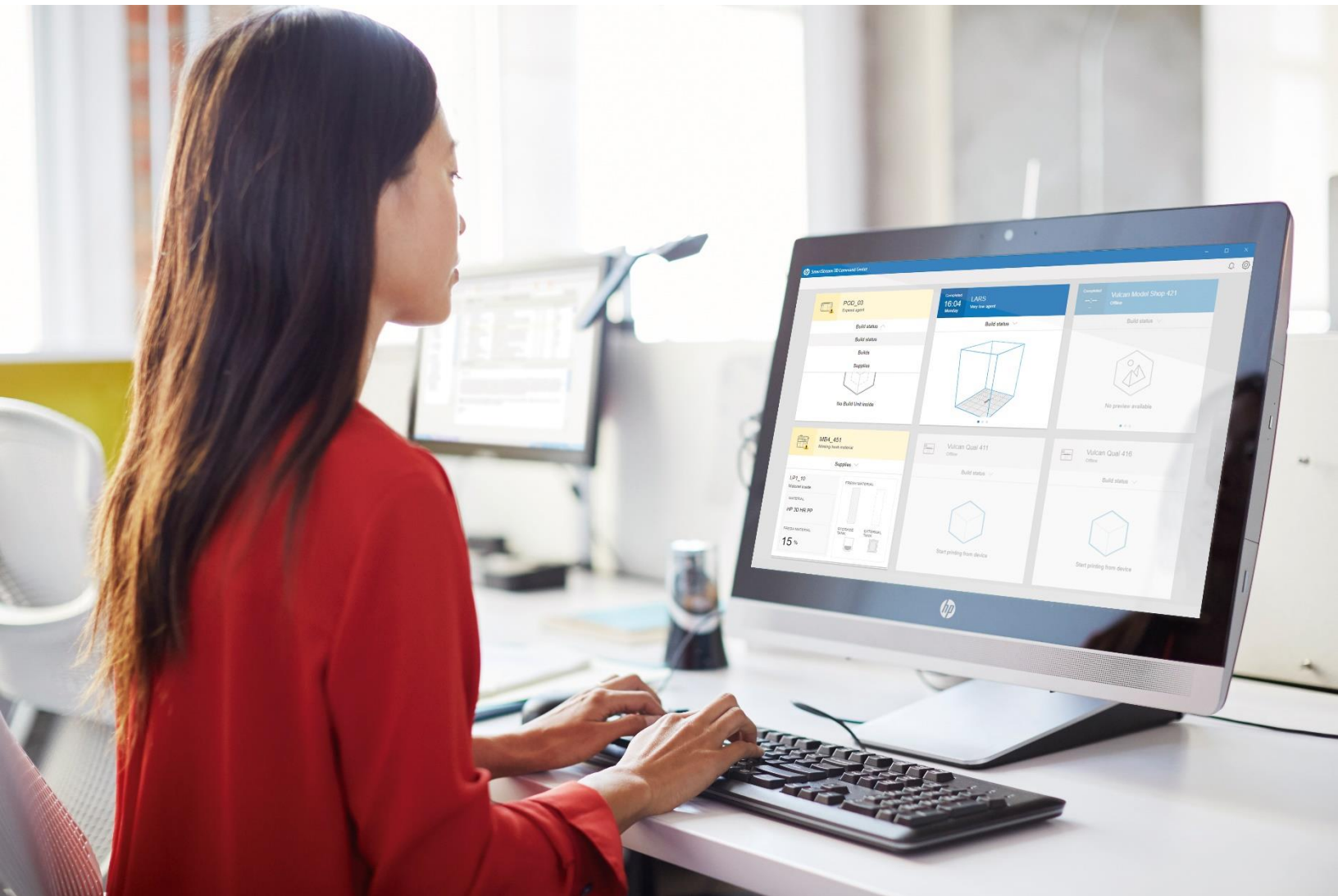




HP SmartStream 3D Command Center 4.0 installation and troubleshooting guide



Contents

CONTENTS	1
DESCRIPTION	3
BENEFITS	3
REQUIREMENTS	4
IT INFORMATION	4
INSTALLATION	6
SERVER INSTALLATION	7
CLIENT INSTALLATION	8
PROXY CONFIGURATION	9
CONNECTIVITY CHECK	11
ADDING DEVICES	11
<i>Device security password</i>	11
<i>Device hostname</i>	13
<i>Create a PrintOS account</i>	14
<i>Log in to PrintOS</i>	15
<i>Add a device in Command Center</i>	18
CONNECTING TO COMMAND CENTER MQTT BROKER	21
CONNECTING TO THE COMMAND CENTER DEVICE API GATEWAY	21
CONFIGURE CUSTOM CERTIFICATES FOR COMMUNICATION BETWEEN COMMAND CENTER AND THE PRINTER	21
UPGRADE PROCESS	22
UPGRADE TO V4.0 OR NEWER VERSIONS	22
UPGRADE TO V3.6 OR NEWER VERSIONS	22
UPGRADE FROM V2.0 OR NEWER VERSIONS.....	23
UPGRADE FROM V1.6	23
UPGRADE FROM V1.5	23
<i>Upgrading all devices at the same time</i>	23
<i>Upgrading the devices progressively</i>	24
<i>Only one PC is available</i>	24
UNINSTALLATION PROCESS	25
TROUBLESHOOTING	26
NETWORK DIAGNOSTICS	26
CONFIGURE COMMAND CENTER TO SUPPORT SSL BUMP FOR TRAFFIC INSPECTION	27
3D PRINTER OR PROCESSING STATION IS OFFLINE IN COMMAND CENTER CLIENT, BUT IT'S TURNED ON	28
EXTRACT DEBUGGING INFORMATION FROM THE COMMAND CENTER SERVER	31
HOW TO VERIFY THAT ALL COMPONENTS ARE RUNNING.....	32
CHECK INTERNET CONNECTIVITY TO PRINTOS, AND BETWEEN COMMAND CENTER SERVER AND CLIENT	33
COMMAND CENTER SERVER APPEAR IN THE LIST, BUT IT'S DISCONNECTED	36
COMMAND CENTER CLIENT IS NOT ABLE TO LOG IN TO PRINTOS.....	36
COMMAND CENTER CLIENT IS NOT ABLE TO CONNECT TO COMMAND CENTER SERVER BACKEND.....	37
COMMAND CENTER CLIENT IS NOT ABLE TO LOG IN TO PRINTOS AFTER PROXY CONFIGURATION	37
CONFIGURING PROXY SETTINGS ON WINDOWS 7	37
DEVICE IS NOT ABLE TO UPLOAD DATA TO THE HP CLOUD.....	38

PROBLEMS CONNECTING TO A SERVER	38
PROBLEMS CONNECTING TO THE COMMAND CENTER MQTT BROKER	39
PROBLEMS CONNECTING TO THE COMMAND CENTER DEVICE API GATEWAY	41
DEVICE MANAGEMENT OR ADD DEVICE BUTTON DOES NOT APPEAR IN COMMAND CENTER CLIENT	44
REMOVE DEVICE BUTTON DOES NOT APPEAR IN COMMAND CENTER CLIENT DEVICE MANAGEMENT	44
APPENDIX	44
ACCESS THE COMMAND CENTER APPLICATION DATA FOLDER.....	44
ACCESSING MOSQUITTO.LOG FILE	46

Description

The aim of this newsletter is to define an easy configuration process for *HP SmartStream 3D Command Center* and to explain which checks should be done to ensure that cloud connection works correctly.

HP SmartStream 3D Command Center consists of two different pieces of software:

- *HP SmartStream 3D Command Center Server* that will communicate with hp cloud.
- *HP SmartStream 3D Command Center Client* where you can add devices and see their status.

Benefits

With this software installed, cloud connectivity is enabled, providing you with the following benefits:

- Remote troubleshooting, minimizing printing downtime.
- Transforming devices into smart devices. This is made possible in part by applying statistical analysis and machine learning techniques to data gathered from connected devices. The installed base of connected devices, combined with cloud intelligence, makes up the HP Jet Fusion 3D Cloud Ecosystem. Improvements may be deployed via device firmware updates or other means.
- Additional functionality, services, and solutions that evolve and improve over time.
- Predictive device maintenance to anticipate required maintenance and part replacement, thereby minimizing printing downtime through planned interventions.
- Machine learning to maximize part quality based on printing parameters and device models that adapt and evolve over time.
- Consistent and predictable part outcomes based on product and process improvement driven from aggregated system telemetry and usage data.
- Productivity. Your production information is always available. Anywhere, anytime access to the status of your HP 3D solutions. HP PrintOS connection enables device status and production parameter monitoring from any web browser or mobile device, from anywhere in the world.
- Monitor KPIs effortlessly. Compare your productivity anonymously to other HP Jet Fusion 3D device users. Productivity data may include packing densities, utilization indices, material recycling percentages, and more.
- Better planning and increased efficiency.

Requirements

- Intel processor with four virtual cores.
- 8 GB of RAM.
- 400 GB of free hard disk space. Ethernet, IPv4, 100 Mb/s.
- Microsoft Windows 10 (64-bit), Windows Server 2012 R2 up to Windows Server 2016.
- Internet connection, ADSL or better.
- Shielded CAT-6 LAN cables to connect the printer and processing station to your LAN.
- Configure firewall or antivirus to allow software to connect to the Internet (HP Cloud).
- This software version is mandatory with devices running firmware versions TATDAG_14_18_05.X or later.
- It is not backward compatible with firmware versions earlier than TATDAG_14_18_05.X, so make sure you also upgrade the firmware to the latest version for all devices after you install this software.
- The maximum number of devices supported by a single Command Center server is 45.

IT Information

- Device Data is accessed through HTTPS from Command Center Server using the Web Services from the devices.
- Data connections to the cloud are always initiated by Command Center Server. No incoming network ports need to be opened on the Internet facing firewall, except for outgoing HTTP traffic, which needs TCP port 443 to be allowed on the network firewall if necessary.
- The PC where Command Center Server is installed needs to be always on and awake to maintain connection with the HP Cloud.
- Neither the HP SmartStream 3D Command Center nor any devices connected to it need to be reached from the Internet.
- HP 3D Printing Solution status and health monitoring require frequent uploads of small data payloads to the HP Cloud (depending on number of devices). Outgoing connections are opened and immediately closed for each payload to reduce any potential security risks.
- Command Center Server uses HTTPS web protocol, but it is not a web browser: it cannot be used to access anything other than the HP Cloud and it is not affected by web browser vulnerabilities.

- Full security audits and vulnerability scans are performed on the Command Center software before release.
- Printers and supporting devices run on dedicated hardware and firmware that is not affected by typical vulnerabilities of personal computers.
- Full security audits and vulnerability scans are performed on HP device firmware before release, and firmware update files are digitally signed by HP and verified by the HP device before installation.
- Device non-anonymous data is never shared with unauthorized 3rd parties without the customer's consent. The HP Cloud stores the device data in HP authorized data centers that meet strict HP security standards, and the system is periodically audited to help ensure the highest level of data security.
- The HP SmartStream 3D Command Center software transmits device data to HP Cloud servers using HTTPS. The identity of the servers is verified, and the communication between the HP SmartStream 3D Command Center software and the HP Cloud servers is encrypted using the Advanced Encryption Standard (AES) algorithm in Cipher Block Chaining (CBC) mode, to ensure that the device data cannot be viewed or modified by any third party.
- Use of hostnames or static IP addresses in devices and the Command Center Server PC is needed to prevent disconnection if the IP changes.
- The Command Center Server PC needs to allow incoming traffic to the Command Center Server application so Command Center Clients can connect to the server.
- Connection to the HP Cloud requires the customer network to allow traffic from the Command Center Server to the following endpoints:
 - Any host at **printos.com**, port 443
 - **3dpconf.heleni.me**, port 443 (or <https://3dpconf.heleni.me>)
 - Any host at **amazonaws.com** port 443
 - Any host at **id.hp.com** port 443 (or <https://directory.id.hp.com>)
 - **h19002.www1.hp.com** port 21 (or <ftp://h19002.www1.hp.com>)
 - **core.api.hp.com** port 443 of (<https://core.api.hp.com>)
- Proxy is taken from the system configuration if not configured in Command Center. But configuration is required to support proxy authentication.

Installation

IMPORTANT: This process is for new users. If you are updating HP SmartStream 3D Command Center, please check the notes on the **Upgrade process**.

The HP SmartStream 3D Command Center Server needs to be installed on a pc that has access to the devices (3D printers or processing stations) and access to the Internet and the HP Cloud.

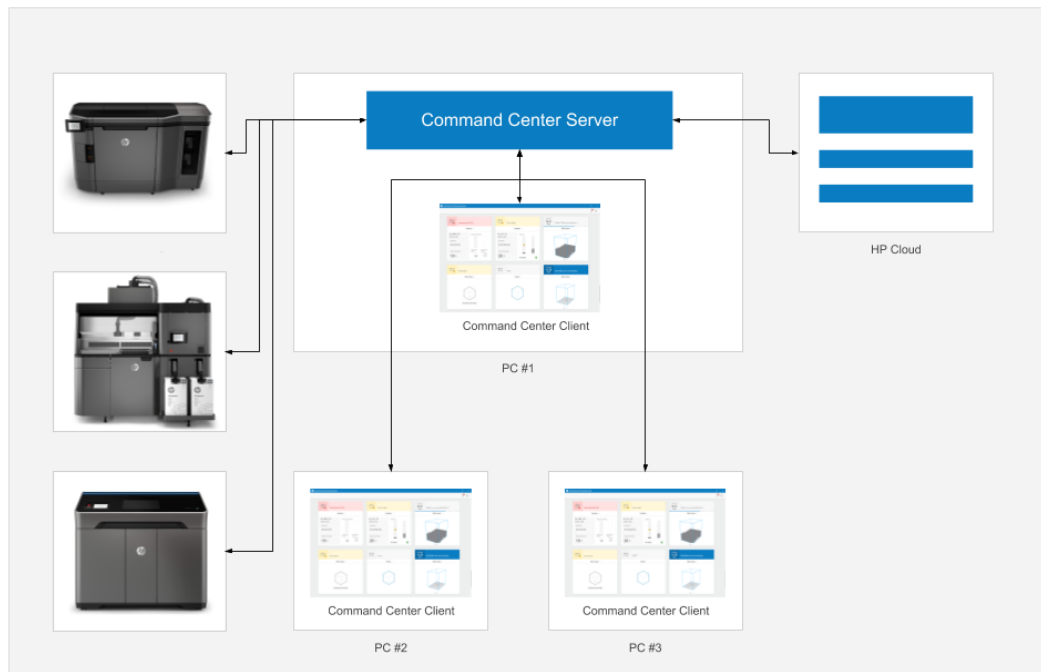
It is necessary to have this PC always turned on to send information from devices to the cloud and to let Command Center Clients monitor the list of configured 3D printers / processing stations. Remember to disable the sleep/standby mode in the PC.

Only one HP SmartStream 3D Command Center Server must be installed on the network to avoid confusion.

You can access the 3D printer / processing station information by installing the HP SmartStream 3D Command Center Client in any pc on your network, provided that the network has access to the main pc where the Command Center Server is installed.

The Command Center Server has no user interface (it just shows the system tray icon), it just contains processes that will run in the background.

The following picture shows a typical configuration where the Command Center Server is running in “Server PC” and the clients can be running in “PC1” or “PC2” or in the same “Server PC”.



IMPORTANT: It is very important to ensure that 3D printers, processing stations, and PCs have the same time zone (reference is UTC/GMT). Check that the PC has correctly configured the date and time, the same as the world official time (http://www.worldtimeserver.com/current_time_in.UTC.aspx).

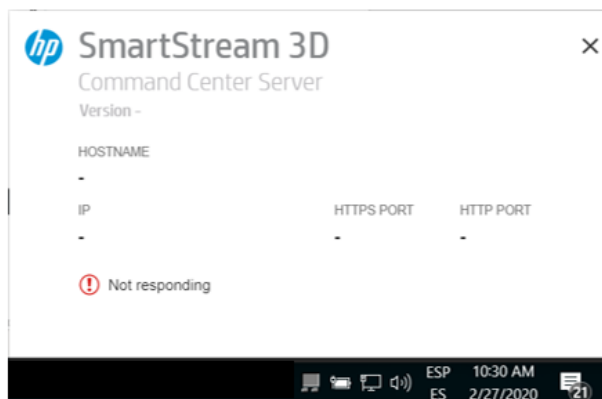
Also, check the “Daylight saving time” is correctly configured (if applicable).

Server installation

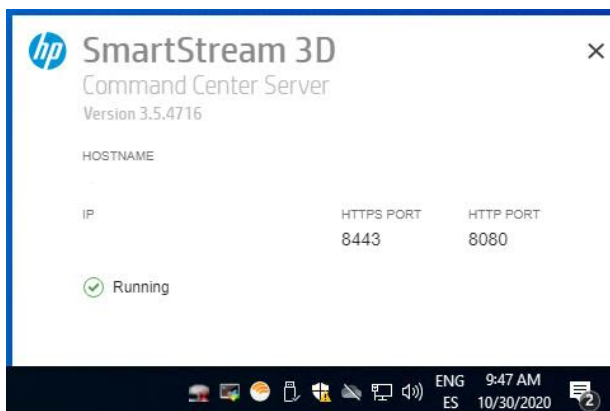
1. Download *HP SmartStream 3D Command Center Server* from the HP website in the support section.
The version must be 4.0.x:
<https://www.hp.com/go/SmartStream3DCommandCenter/software>.
2. Install *HP SmartStream 3D Command Center Server* only once on the current network, on the server PC.
3. Check the status of the *HP SmartStream 3D Command Center Server* with the server tray icon in the system tray, situated at the bottom-right corner. The server tray has the same icon as the *HP SmartStream 3D Command Center* application.

You may encounter the following issues:

- The server is not responding.



- The server is running and using the correct ports.

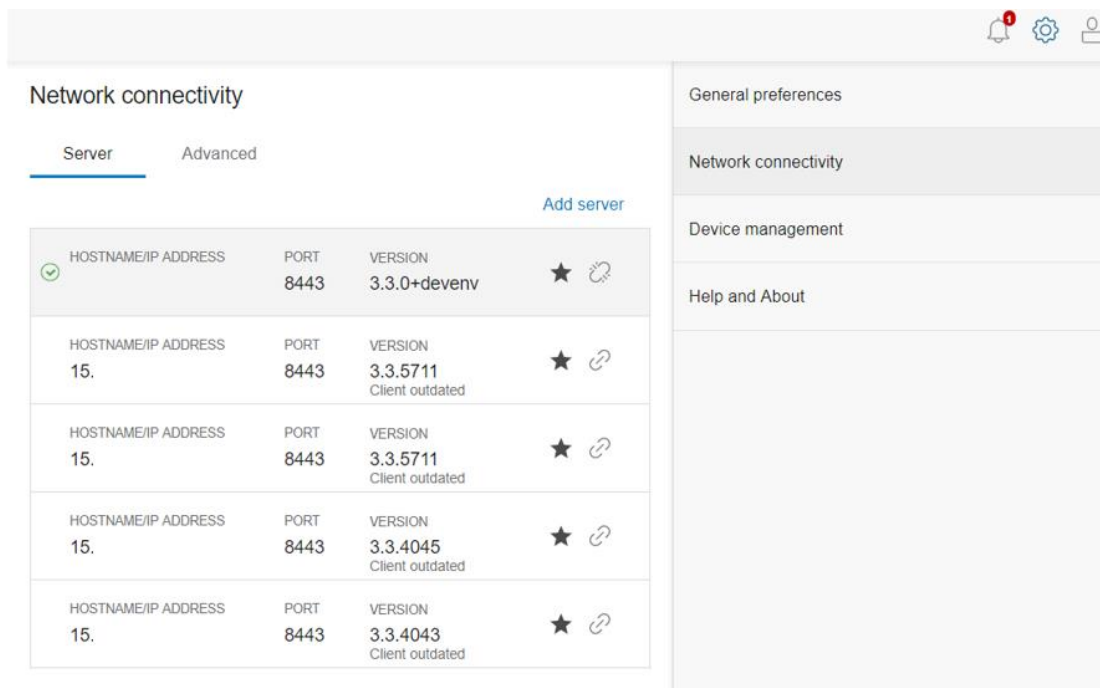


Client installation

1. Download *HP SmartStream 3D Command Center Client* from the HP website in the support section.
The version must be 4.0.x:
<https://www.hp.com/go/SmartStream3DCommandCenter/software>.
2. Install *HP SmartStream 3D Command Center Client* in all the computers where you want to see the status of your devices. It is recommended to install it also on the server PC.
3. Open *HP SmartStream 3D Command Center Client* and click the gear icon at the top-right corner, and then click **Network connectivity**.
4. Verify there is a valid server found:

IMPORTANT: From version 3.2 of Command Center, HTTPS connection has been enforced. Thus, now only secured servers (with HTTPS) will be autodetected, this means that all servers with a version earlier than 3.2 will not be discovered. In addition, non-secured connections to servers (without https, port 8080) cannot be added manually.

- a. If the server is detected automatically it will show the server IP address directly. The client will be connected automatically to the autodetected server if there is just one. Otherwise, you should select the desired server to connect to. You can save autodetected servers to favorites by clicking the star.
- b. If it does not appear in the server list, you can add it manually with the “Add Server” option. Include the server IP address and port (from 8443 to 8449). The IP and the port are also displayed in the tray icon.



IMPORTANT: Remember that it is strongly recommended to configure a static IP address rather than a DHCP address for the “Server PC” to allow Command Center Clients to always find the Command Center Server, as the IP can change in DHCP environments when no MAC reservations are configured for the device.

Proxy configuration

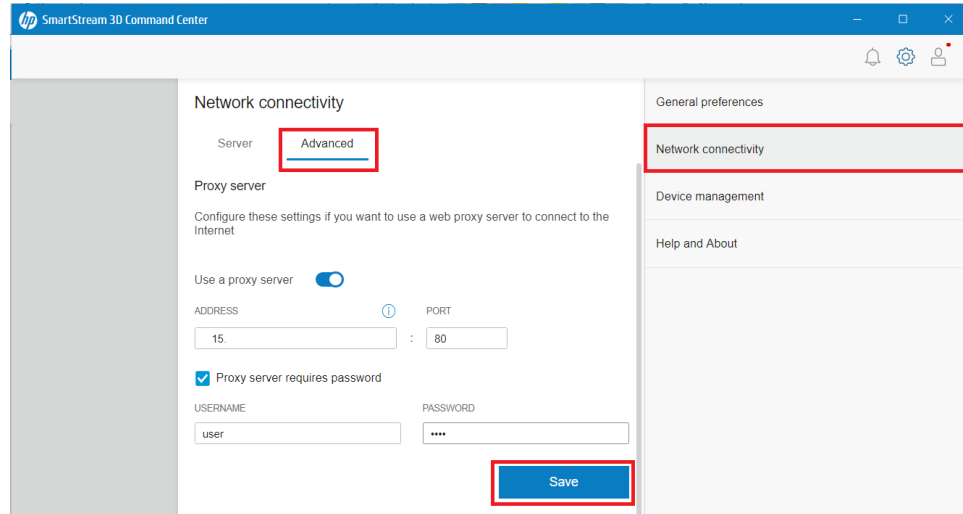
In case it is necessary to configure the Internet connection via proxy server:

1. Open *HP SmartStream 3D Command Center Client* and click the gear icon at the top-right corner. And then click **Network connectivity**.
2. You should stay connected to the server to save your configuration.



3. Click the **Advanced** tab.
4. Enable the option **Use a Proxy Server**.
5. Fill in the hostname or IP, and the port of your proxy. If authentication is needed, please add the username and password.

6. Click **Save** to finish the configuration and send it to the *HP SmartStream 3D Command Center Server*.



In addition, the range of the local IP addresses should be added to the local PC proxy configuration, to avoid resolving them through the proxy.

Manual proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Use a proxy server

On

Address

Port

Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries.

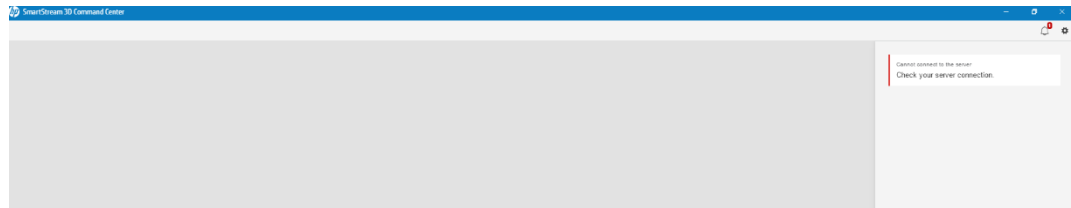
Don't use the proxy server for local (intranet) addresses

IMPORTANT: To ensure correct operation, it is very important to allow proxy connectivity with the Command Center Server (port range 8443-8449 and 8080-8099). If, after proxy configuration, the Command Center Client behaves unexpectedly, or you cannot log in with PrintOS please check the notes in the section **Command Center Client is not able to log in to PrintOS after proxy configuration**

Connectivity check

1. Open *HP SmartStream 3D Command Center Client* and click the gear icon at the top-right corner.
2. You should be connected to your server. If not, click **Network connectivity** and connect.
3. Check that you don't have any connectivity issues by clicking the bell icon at the top-right corner.

If you have issues, first fix them. Check that your network is not blocking our HP Cloud connections.



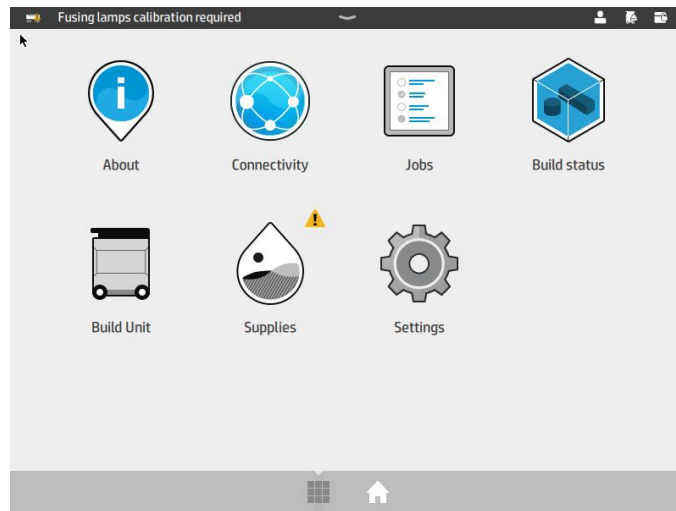
4. To find out more about connectivity issues, go to the Troubleshooting section: **Network Diagnostics** in this document.

Adding devices

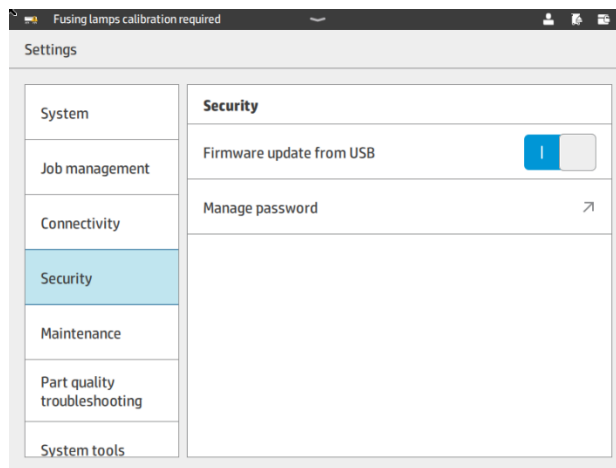
Device security password

You must configure the device security password to be able to associate the device to your Command Center.

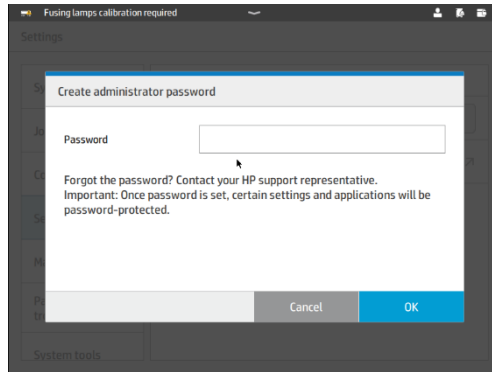
1. Go to the device and enter the **Settings** menu on the device front panel.



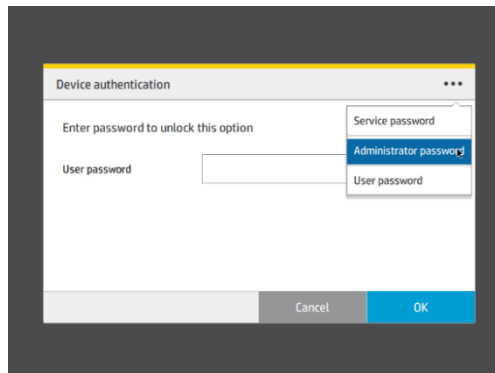
2. Select **Security** settings and then **Manage password**. If you cannot see this screen, it is probably because a password has already been set, in this case go to step **Error! Reference source not found.**



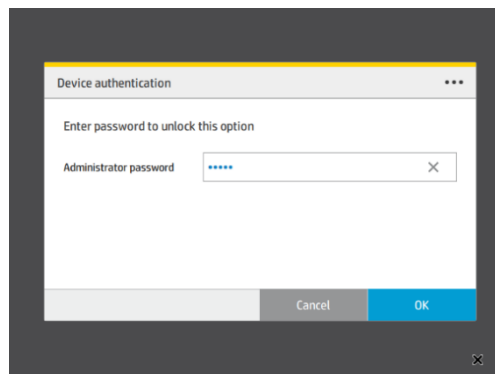
3. Create the administrator password. It is very important to remember this password as you will need it to access certain settings and if you need to add the devices to the Command Center again in the future. If you forget this password, you will need a service intervention to reset it.



If the device already has a password set, you will see this screen instead.



4. Select the three-dot ... icon and choose **Administrator password**. Type the administrator password to check and click the **OK** button:

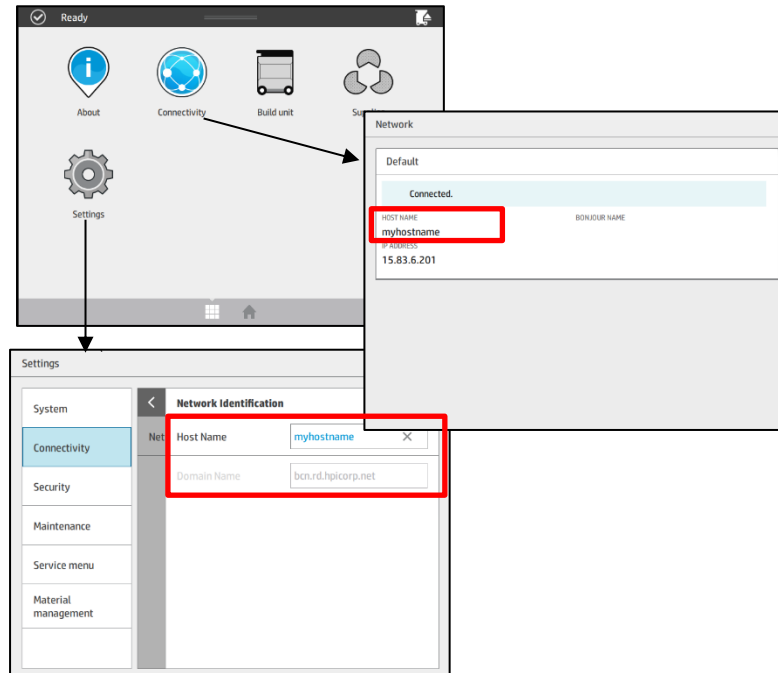


If you don't remember the password, you will need a service intervention to reset the password.

Device hostname

1. You must use a hostname or static IP address for the devices.
You can get the pre-assigned hostname in the connectivity application on the device front

panel, going to: **Settings menu → Connectivity → Network → Gigabit Ethernet → Network Identification → Host Name**



2. In some networks, you also need to add the domain name to the hostname to identify the device. You can find the domain name in the connectivity application on the device front panel, going to:

Settings menu → Connectivity → Network → Gigabit Ethernet → Network Identification → Domain Name

The final domain name in that case will be “hostname.domainName”.

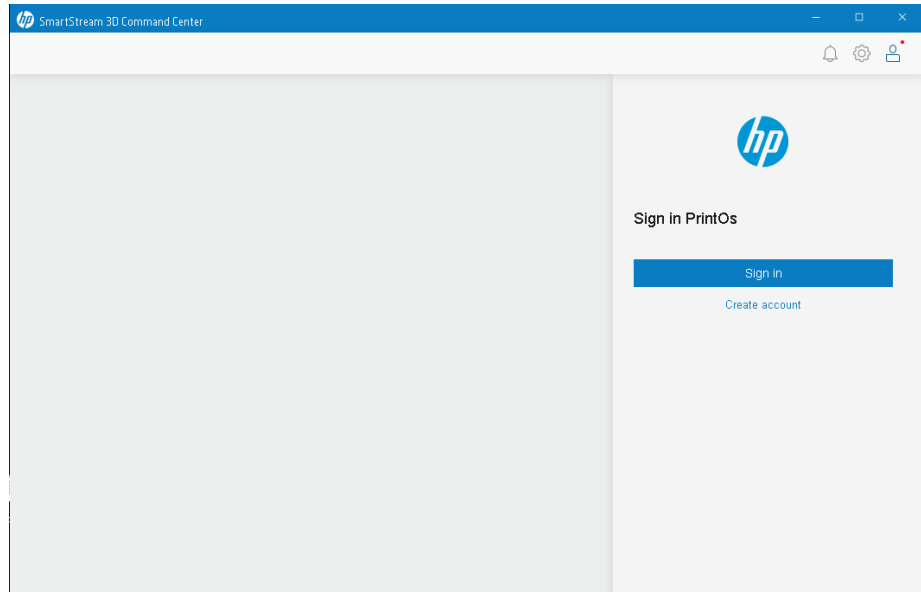
Create a PrintOS account

If you already have a PrintOS account, you can ignore this section.

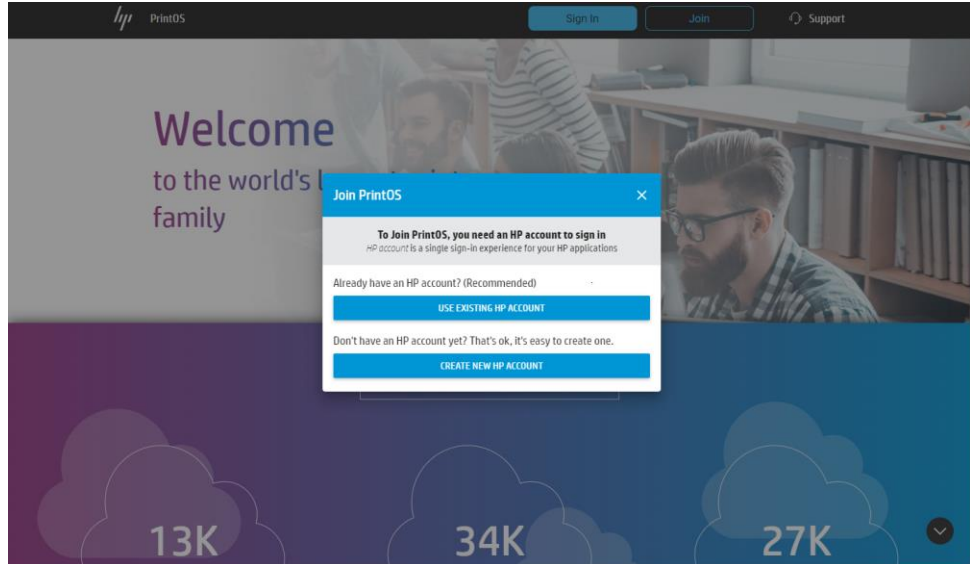
To create a new Customer PrintOS account:

1. In Command Center Client click the user icon at the top-right corner of the window, then click **Create account**.

Note: If the button is not visible, check the connection with the Command Center Server on the Network connectivity panel, as there will be a problem with it.



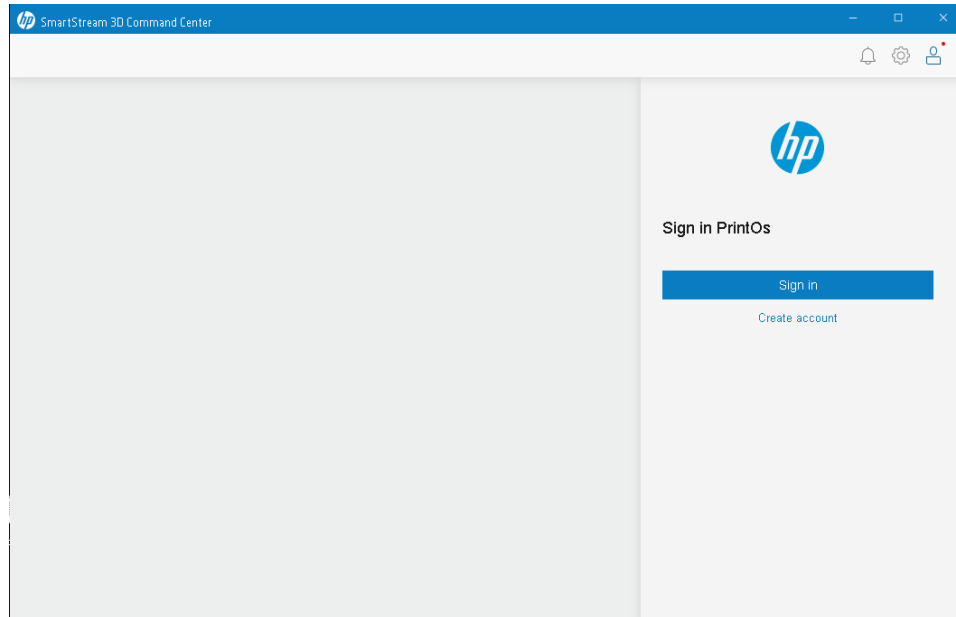
2. You will be redirected to a PrintOS page on the browser. You'll need an HP account to access PrintOS. click **Create new HP account** and fill the fields with your information, then you will receive a verification email. After verification, you'll need to accept the terms & conditions. Once logged in, create an organization using HP 3D as the printer family.



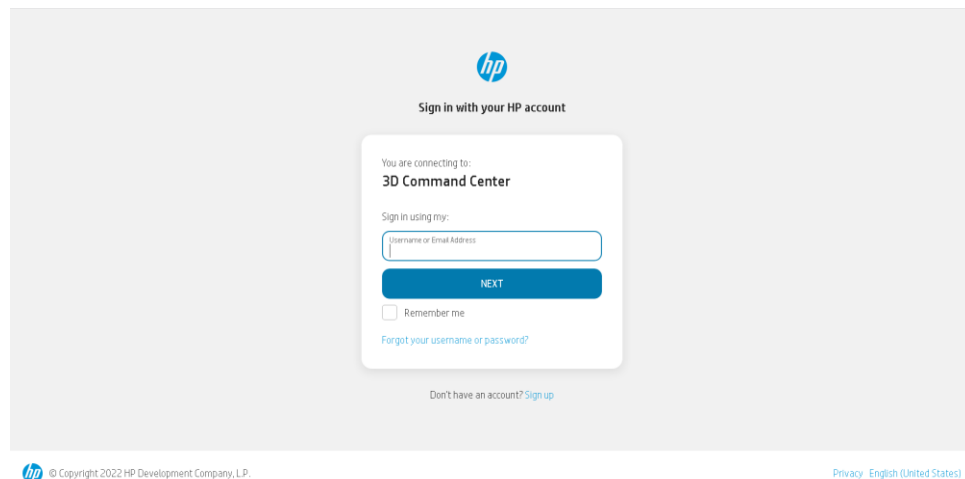
Log in to PrintOS

You must be logged in with your PrintOS account to view and manage your devices.

1. To log in, in Command Center Client click the user icon at the top-right corner of the window, then click **Sign in**. The red ball in the user icon indicates that the user is not logged in.

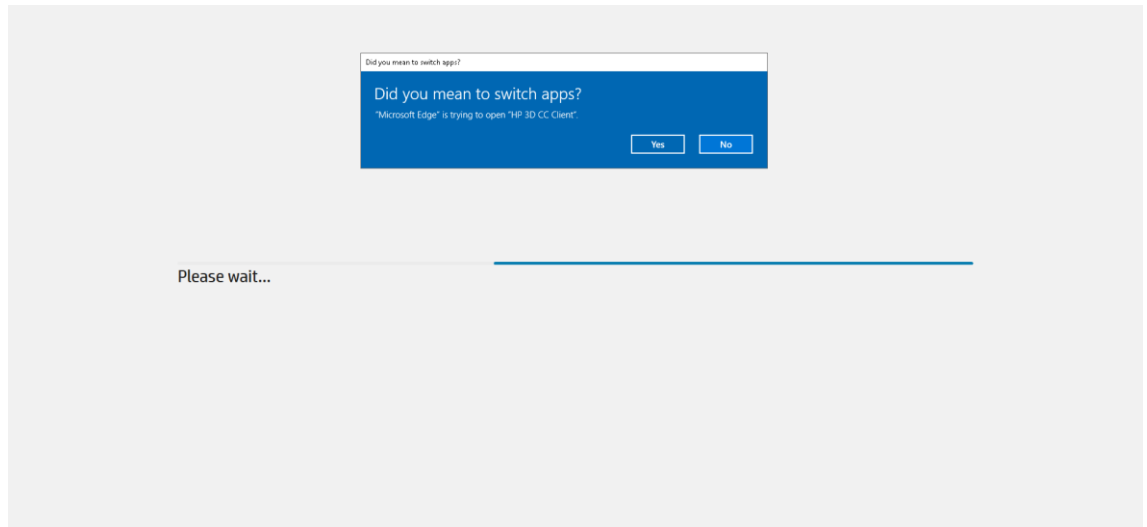


2. You will be redirected to the 3D Command Center login page in your default browser. Fill in your username and password to continue. Generally, the username is the email used in the PrintOS registration. Also, if a user does not remember their username or password, there is a **“Forgot your username or password”** link to help to reset it.

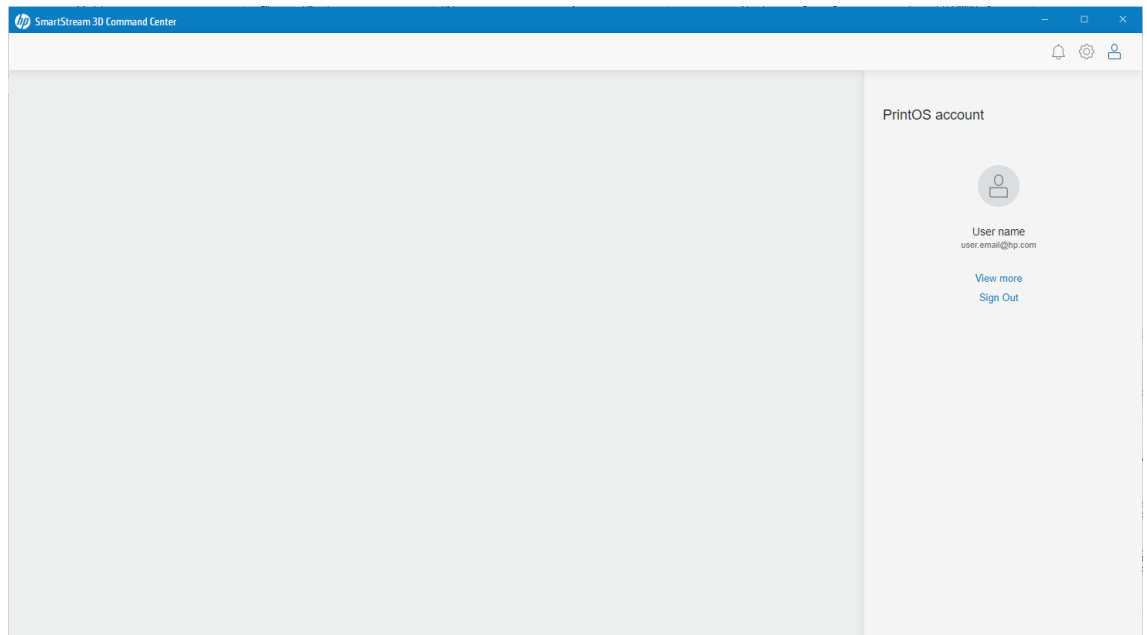


3. After login, a message box will appear in the browser to switch to the Command Center application. You must accept this message box to complete the login process.

Note: The format of this message box may be different depending on your default browser.



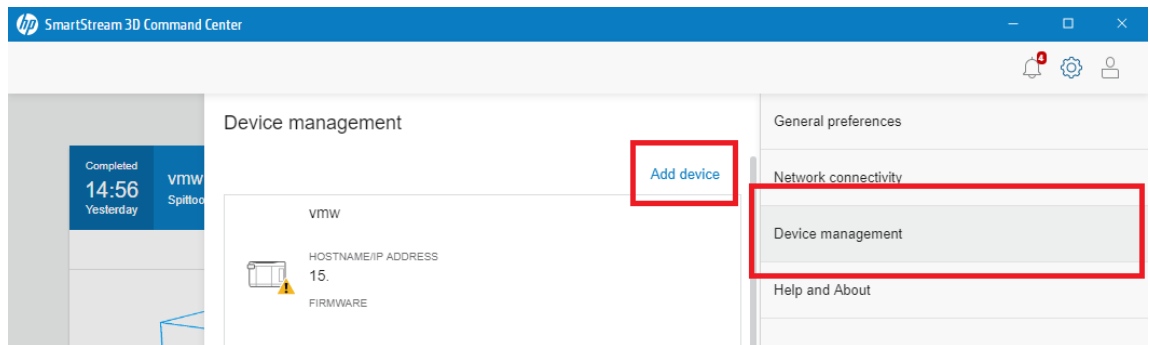
4. Now, the login panel has been replaced with the user information; basically name, surname, and email address registered in PrintOS. Finally, the red ball is no longer visible, which means that there is a user logged in. We can log out using the "Sign Out" link.



Add a device in Command Center

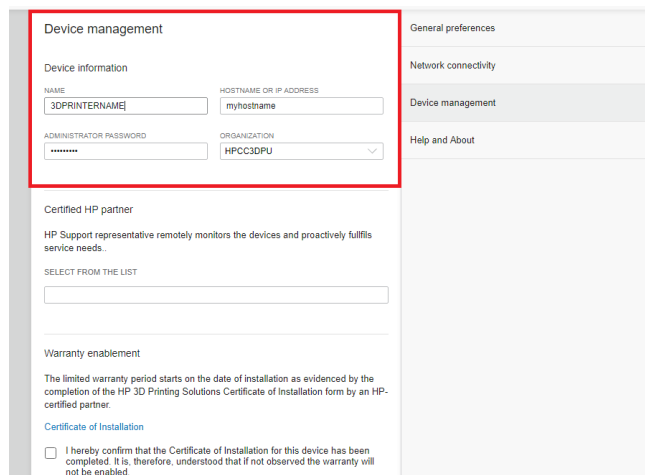
To add a device, it is necessary to log in to PrintOS beforehand. Only PrintOS organization administrators can add devices. Otherwise, the Device Management panel is disabled and cannot be accessed.

1. In Command Center Client go to **Settings → Device Management**, and click the **Add device** button.



Note: If the **Add Device** button does not appear or Device Management is disabled, check the connection with the Command Center Server in the notification center, and login status in the user panel, as there will be a problem.

2. Input a name to identify the device, introduce the static IP, the FQDN, or the hostname (limited to 32 characters) of the device, and the administrator password configured previously through the front panel of the device (check the section in this document on the Device security password) and finally choose the correct organization (if you belong to more than one).

A screenshot of the 'Device management' form. The form is divided into several sections. The 'Device information' section is highlighted with a red box and contains the following fields: 'NAME' with a text input field containing '3DPRINTERNAME', 'HOSTNAME OR IP ADDRESS' with a text input field containing 'myhostname', 'ADMINISTRATOR PASSWORD' with a password input field containing '*****', and 'ORGANIZATION' with a dropdown menu showing 'HPCC3DPU'. Below this, there is a 'Certified HP partner' section with a checkbox and a 'Warranty enablement' section with a checkbox and a 'Certificate of Installation' section with a checkbox.

Command Center doesn't support using a DHCP server to handle the device IP unless it is through MAC reservations. If a dynamic IP address is used, when it changes the connectivity with the Command Center will be lost, and you will need to remove and add the device each time it changes.

- 3. From the list, select the Certified HP partner that installed your devices.

The screenshot shows the 'Device management' page. Under 'Device Information', there are fields for 'NAME' (3DPRINTER), 'HOSTNAME OR IP ADDRESS' (myhostname), and 'ADMINISTRATOR PASSWORD' (masked with asterisks). Below this is the 'Certified HP partner' section, which is highlighted with a red box. It contains the text: 'HP Support representative remotely monitors the devices and proactively fulfills service needs.' and a dropdown menu labeled 'SELECT FROM THE LIST' with the value 'HP Inc. 3D-SWQAR'. Below that is the 'Warranty enablement' section, which includes a checkbox and text: 'I hereby confirm that the Certificate of Installation for this device has been completed. It is, therefore, understood that if not observed the warranty will not be enabled.'

- 4. Now check the Warranty and Certificate of installation. Please take care of this to enable your warranty for the device.

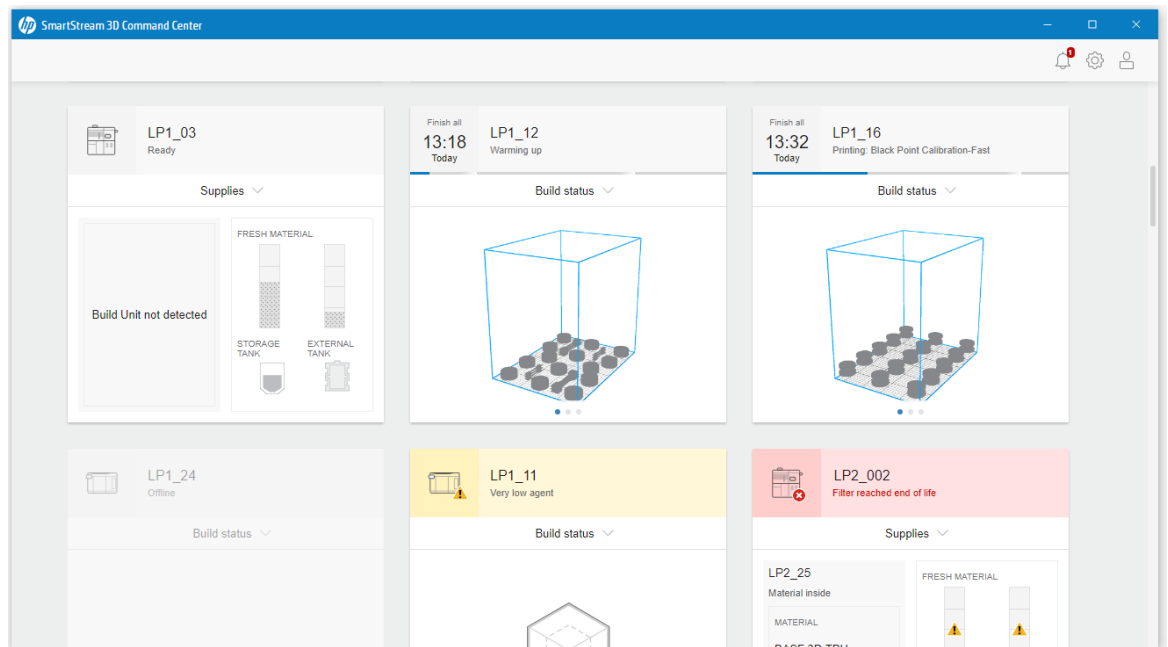
The screenshot shows the 'Device management' page. Under 'Device Information', there are fields for 'NAME' (3DPRINTER), 'HOSTNAME OR IP ADDRESS' (myhostname), 'ADMINISTRATOR PASSWORD' (masked with asterisks), and 'ORGANIZATION' (a dropdown menu). Below this is the 'Certified HP partner' section, which is empty. Below that is the 'Warranty enablement' section, which is highlighted with a red box. It contains the text: 'The limited warranty period starts on the date of installation as evidenced by the completion of the HP 3D Printing Solutions Certificate of Installation form by an HP-certified partner.' and a checkbox with the text: 'I hereby confirm that the Certificate of Installation for this device has been completed. It is, therefore, understood that if not observed the warranty will not be enabled.'

5. Click the **Save** button. Now your device has been added to the Command Center. You need to check that there is no warning in the notification center to be sure the device has been correctly installed. Repeat the process if you need to add more devices.

Possible error output messages in this step:

- “Invalid device name” message:
 - Name of the device is not valid. Some characters are not supported.
- “Invalid device credentials” message:
 - Device admin password is incorrect.
- “Device not supported” message:
 - PrintOS account does not belong to a 3D account or invalid device serial number.
- “Device already associated to another PrintOS account” message:
 - Device is registered to another customer, or you are using a different PrintOS account.
- “Admin credentials not configured” message:
 - You need to set an admin password for the printer and processing station. Refer to the section **Device security password**.
- “Error while adding a device. Try again XXXX”
 - This is a generic error message for errors that the Command Center has not contemplated, being XXXX the code reported by PrintOS.

6. After adding all devices, you will end with a screen like this:



Connecting to Command Center MQTT broker

To connect to the MQTT broker, you will need to use the following settings:

- *Protocol*: mqtt://
- *Server_IP*: IP of the server, which is shown in the tray icon.
- *Port*: It can be checked by getting the server discovery in the following way:
`GET https://<Server_IP>:8443/discovery`

The default port is 1883, but if it is busy a port in the 1883-1891 range will be chosen.

You can check the names of the topics reported through MQTT with the trace 3DSSCCDC.log: "Data has been posted". The metadata of this trace contains the response of the printer after enabling the topics. There, you will find a summary of the topics that have the MQTT enabled.

To register as a client for the different topics:

- Register to "#" to receive all topics.
- Register to individual topics in the following way: `+/+/telemetry/<Topic name>`
i.e.: `+/+/telemetry/Public/DeviceInformation/Identification`

If you experience problems connecting to the MQTT broker, go to the troubleshooting section:

Problems connecting to the Command Center MQTT Broker.

Connecting to the Command Center device API gateway

Users should follow the instructions given in the following resource:

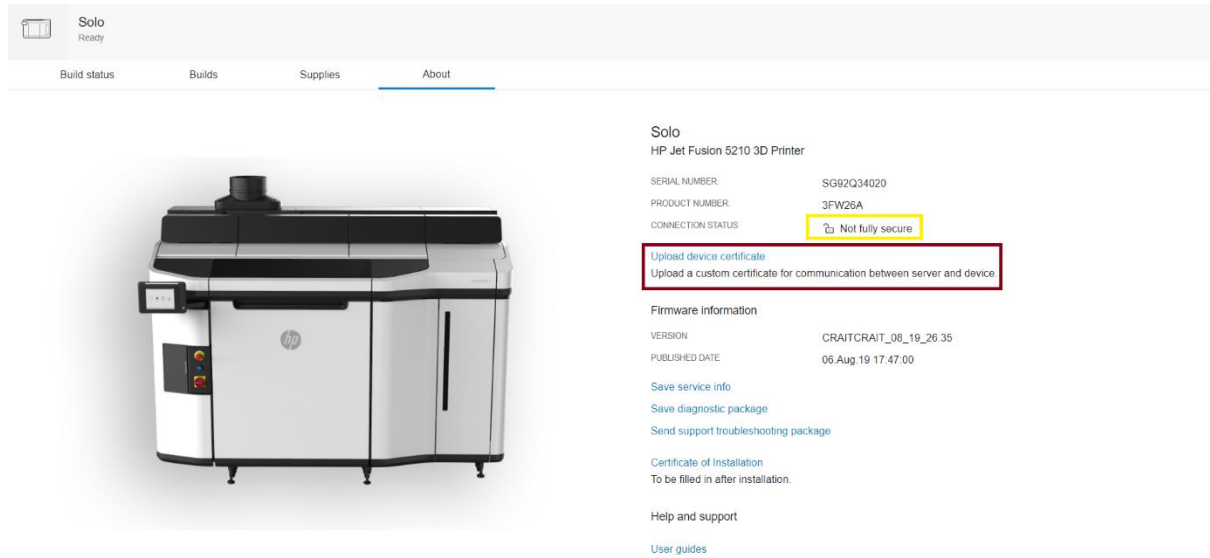
<https://developers.hp.com/3d-printing-apis/multi-jet-fusion-api-specifications>

Configure custom certificates for communication between Command Center and the printer

HP printers come with a self-signed certificate to create the HTTPS connections between the printer API and HP software or HP partner's software.

You may want to replace this certificate for one signed by a publicly trusted certificate authority (CA) or your company private CA. To do this select or change the hostname of the printer to the one that you want to use inside your network. Then you can create the certificate signing request (CSR) with the hostname, it is recommended also to add the static IP of the printer in the subject alternative name, so it supports adding the printer to Command Center using IP instead of hostname.

Once you have the proper CSR you can sign it using a publicly trusted CA or your company private CA. The signed certificate should be uploaded to the printer using the **Upload device certificate** button in **Command Center > Device > About**:



If you previously added the printer to Command Center using a static IP and forgot to add the subject alternative name, you should go to **Command Center > Settings > Device management** and remove the printer and add it again using the same hostname you used in the certificate.

If you used your company private CA, you should add the public certificate of the origin of trust to the Command Center so it can trust the certificate signed by this CA. You should export the public certificate of your root CA in Base-64 encoded (.CER) to the user-certificates folder in the Application directory, see full path:

```
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\HP\3D  
SSCC\user-certificates
```

Restart the server. Once the Command Center server processes start again, it will load this certificate, and the certificates signed by this entity will be trusted.

Upgrade process

Upgrade to v4.0 or newer versions

When an upgrade to v4.0 from older versions takes places. Take into account that when you update your Command Center, until the frontend is updated you will be logged out from PrintOS, and you will not be able to log in until Command Center Client is updated. The devices may also appear as offline.

Upgrade to v3.6 or newer versions

When an upgrade to v3.6 from older versions takes places. Take into account that when you update your Command Center, you will be logged out from PrintOS.

Upgrade from v2.0 or newer versions

There are no special requirements to upgrade Command Center from these versions. Follow the steps in the sections **Installation → Server installation** and **Installation → Client installation**. Your devices and proxy configurations will be preserved.

Upgrade from v1.6

You must follow these steps to avoid installer failures:

1. Uninstall previous Command Center Server and Clients.
2. Reboot the PC.
3. Install the new version of Command Center Server and Client.

Your devices and proxy configurations will be preserved.

Upgrade from v1.5

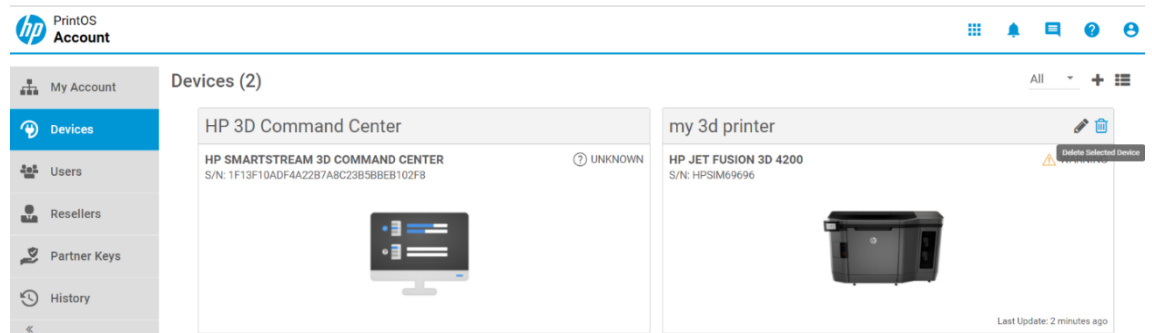
On the current version, the minimum firmware version for the devices is: TATDAG_14_18_05.X.

If you need to upgrade your firmware, check your scenario:

IMPORTANT: Consider that due to security improvements in the application, the installation of Command Center 1.6 or later will automatically remove all the devices you had previously added, and you will need to add them again.

Upgrading all devices at the same time

1. Uninstall the previous Command Center server and Client version and reboot the PC.
2. (Step needed only if you are upgrading to model 4210) Remove the devices from the PrintOS account as the product number will change. You need to log in to your PrintOS customer account with your web browser (www.printos.com) and remove the device by clicking the trash (🗑️) icon.



3. Upgrade devices (printers and processing stations) to firmware TATDAG_14_18_05.X or latest.
4. Install the new Command Center Server and Client version (all devices are deleted by default).
5. Add devices to Command Center (important to add devices once migrated to the new firmware version. If you add a device with older firmware versions, you **MUST** remove it from Command Center and add it to Command Center again once migrated to the new firmware version).

Upgrading the devices progressively

Another PC is available - Recommended by HP

1. Install the new Command Center Server and Client version in the second PC (PC2).
2. *(Step needed only if you are upgrading to model 4210)*. Remove the devices from the PrintOS account as the product number will change. You need to log in to your PrintOS customer account with your web browser (www.printos.com) and remove the device by clicking the trash icon (🗑️).
3. When upgrading a device to firmware version TATDAG_14_18_05.X or later, remove the device from the old Command Center in PC1 and add the device to the new Command Center in the second PC (PC2).
4. Once all devices have been migrated to the new firmware version, remove the old Command Center in PC1.
5. *(Optional)* If you want to keep PC1 as the server PC for Command Center, uninstall Command Center in PC2 and install the new Command Center in PC1 and add all the devices again (all of them **MUST** have been migrated to the new firmware version).

Only one PC is available

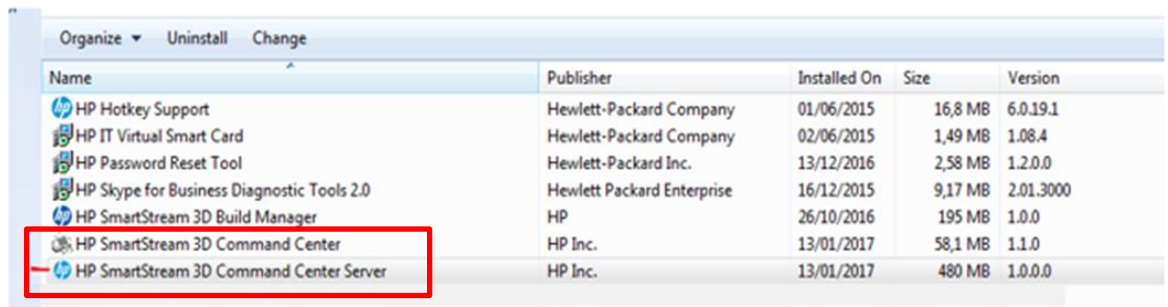
1. Uninstall the previous Command Center Server and Clients and reboot the PC.
2. Upgrade some of the devices to firmware version TATDAG_14_18_05.X or later.
3. Install the new Command Center Server and Client version.
4. Add all the devices to Command Center (with older and new firmware versions).
5. When a device is upgraded to the new firmware version, remove it from Command Center, upgrade the firmware and then add it to Command Center again (credentials will refresh to enable correct sending of the information). If not done, the device won't be connected correctly to the cloud and printing / powder loading will stop working.

IMPORTANT: Avoid adding TATDAG_14_18_05 firmware devices to HP SmartStream Command Center versions earlier than 1.6 as devices won't be correctly connected to the cloud and printing / powder loading will stop working.

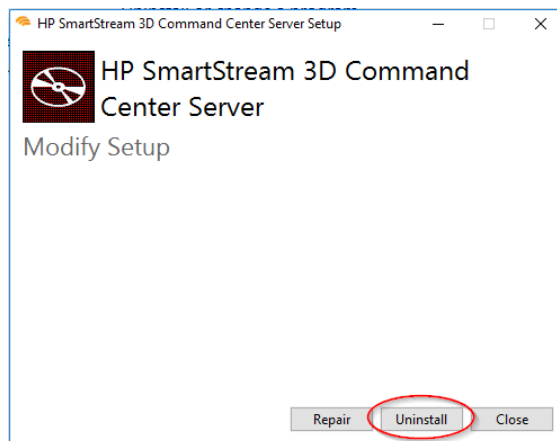
Remember to remove the device from the Command Center and add it again after the upgrade of the device to firmware version TATDAG_14_18_05.X as devices won't be correctly connected to the cloud and printing / powder loading will stop working.

Uninstallation process

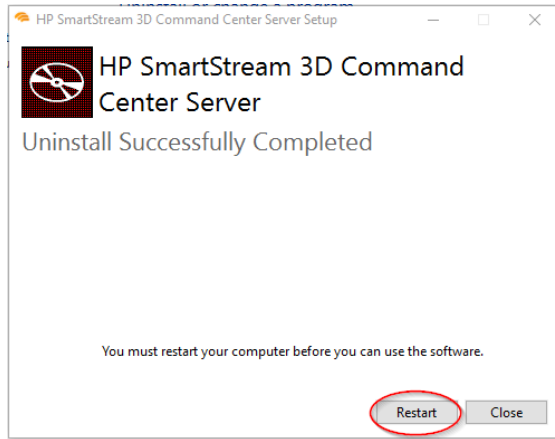
1. Uninstall the previous version of the Command Center Server/Client. To do this, on the “Server PC” access **Control Panel** → **Program and Features** and then locate the “HP SmartStream 3D Command Center Server” and “HP SmartStream 3D Command Center”, and click **uninstall**. The first one will uninstall the server and the second one the client.



2. To uninstall the server, click the **Uninstall** button in the dialog box.



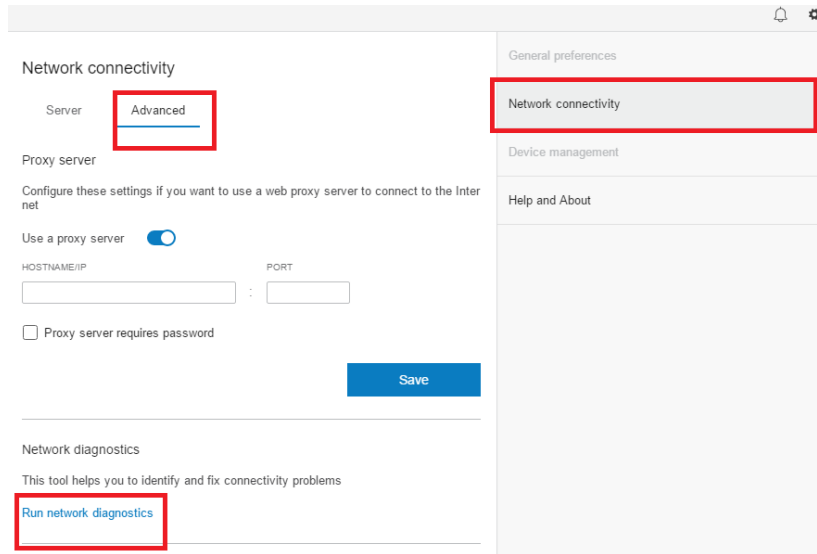
2. Reboot the PC (required if you need to install the software again).



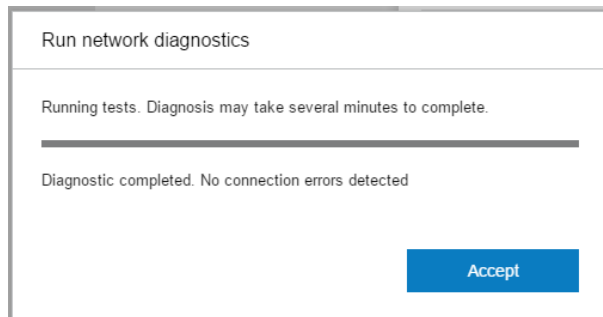
Troubleshooting

Network diagnostics

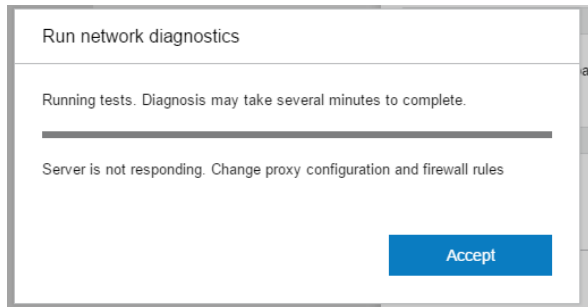
If you need to identify connectivity problems, you can run network diagnostics.



If no error is detected, you will receive:



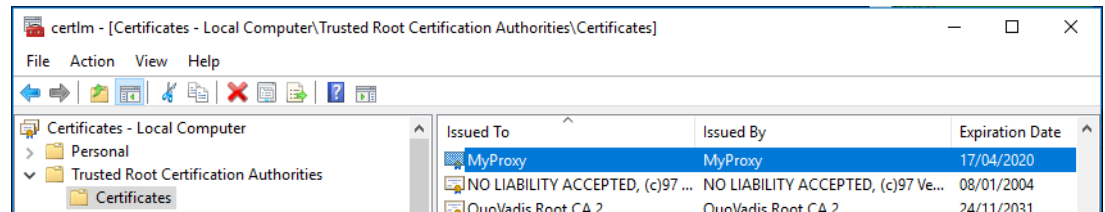
If errors are detected, you will receive different error messages depending on the cause:



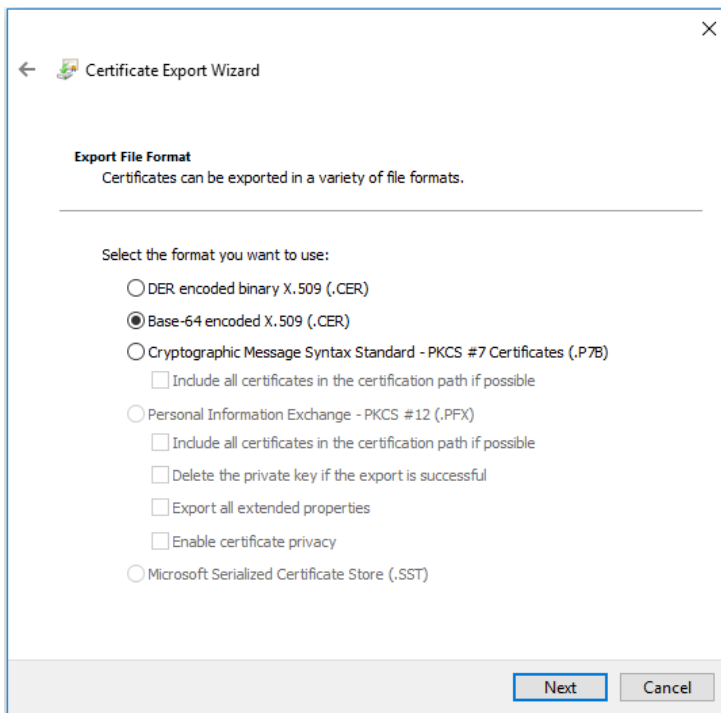
Configure Command Center to support SSL Bump for traffic inspection

You must add the public certificate from the SSL inspector that is used to generate the ad-hoc certificates for all sites (so the real ones can be swapped). Once you add this certificate to the Command Center Server, it will start to trust the encrypted traffic from the SSL inspector.

Open the local computer certificate console (certlm.msc) and check whether the public certificate of the device performing the SSL inspection is already added to the Trusted Root Certification Authorities folder. If not, please add it.



If already added to the local certificate store, export it as Base-64 and save the file. If you have any trouble to identify the certificate, please ask your IT department for assistance.




Move the exported certificate to the user-certificates folder in the application directory, see full path:

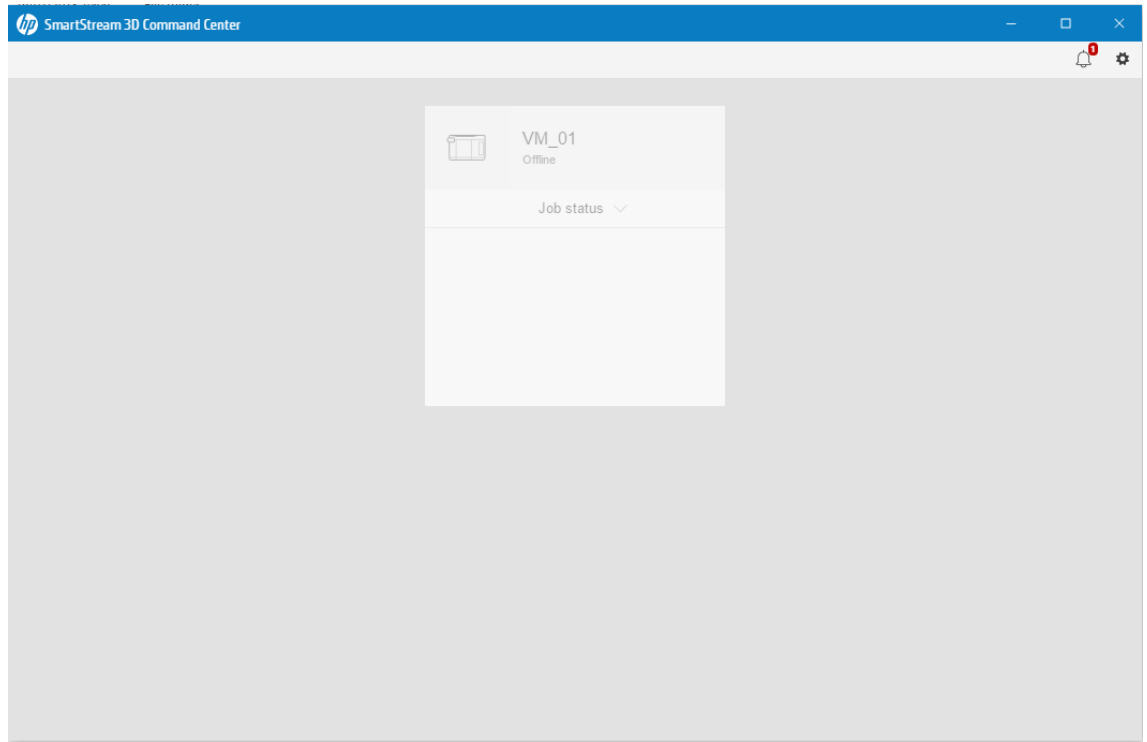
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\HP\3D SCCC\user-certificates

Restart the server. Once the Command Center server processes start again, it will load this certificate, and the traffic from the SSL/TLS inspector will be trusted as if it was unencrypted.

3D Printer or Processing Station is offline in Command Center Client, but it's turned on

Symptom: The IP of the device has probably changed. To avoid this kind of problem, configure a static IP address, FQDN or hostname as explained in the installation instructions.

You can also check the connectivity icon () for any warning that the Command Center software is not connected to the device:

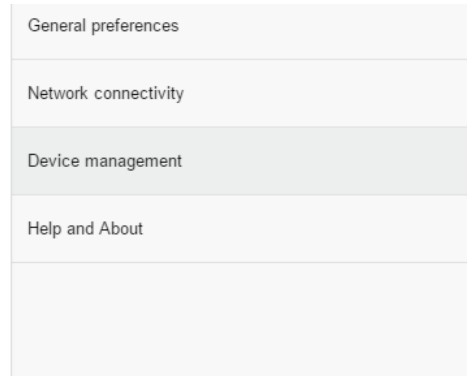
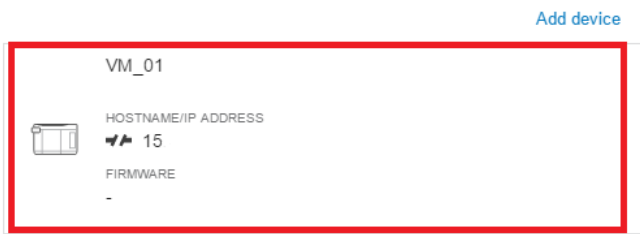


Solution: Once HP SmartStream 3D Command Center Client is launched, click the gear icon at the right side of the window:

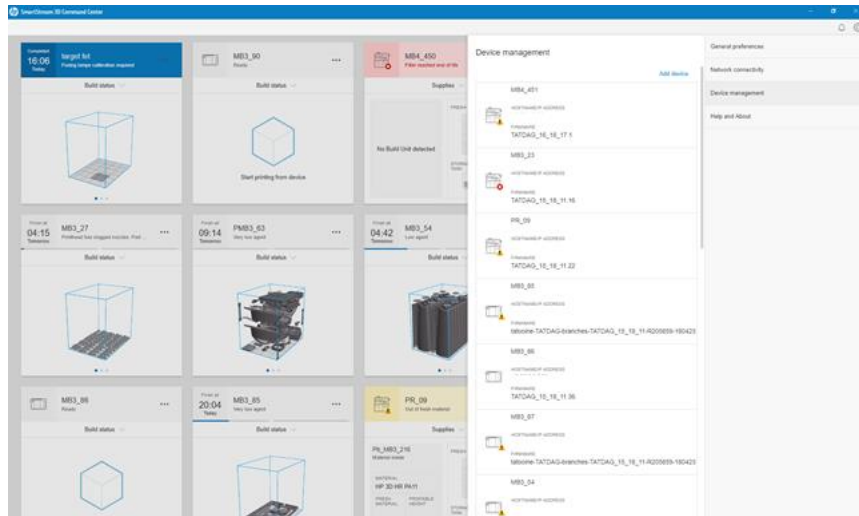


After this, a pop-up window appears. In the section corresponding to device management, it should list the hostname/IP address of the 3D printers and processing stations. If the hostname/IP address doesn't appear or there is a disconnected icon, it means that Command Center can't reach the device:

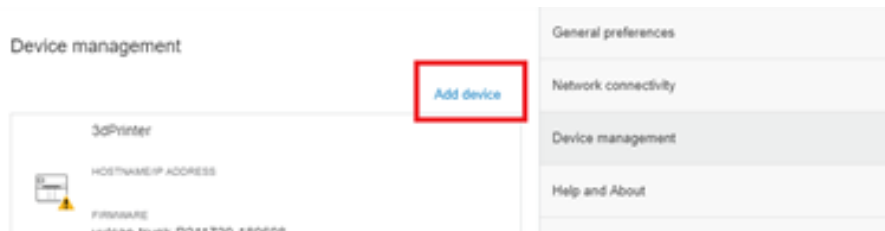
Device management



In this picture 3D printers and processing stations are correctly connected:



Please delete the device by clicking the trash icon, and then add it again (using a static IP address, FQDN or hostname) by clicking the **Add device** link at the bottom of the dialog box:



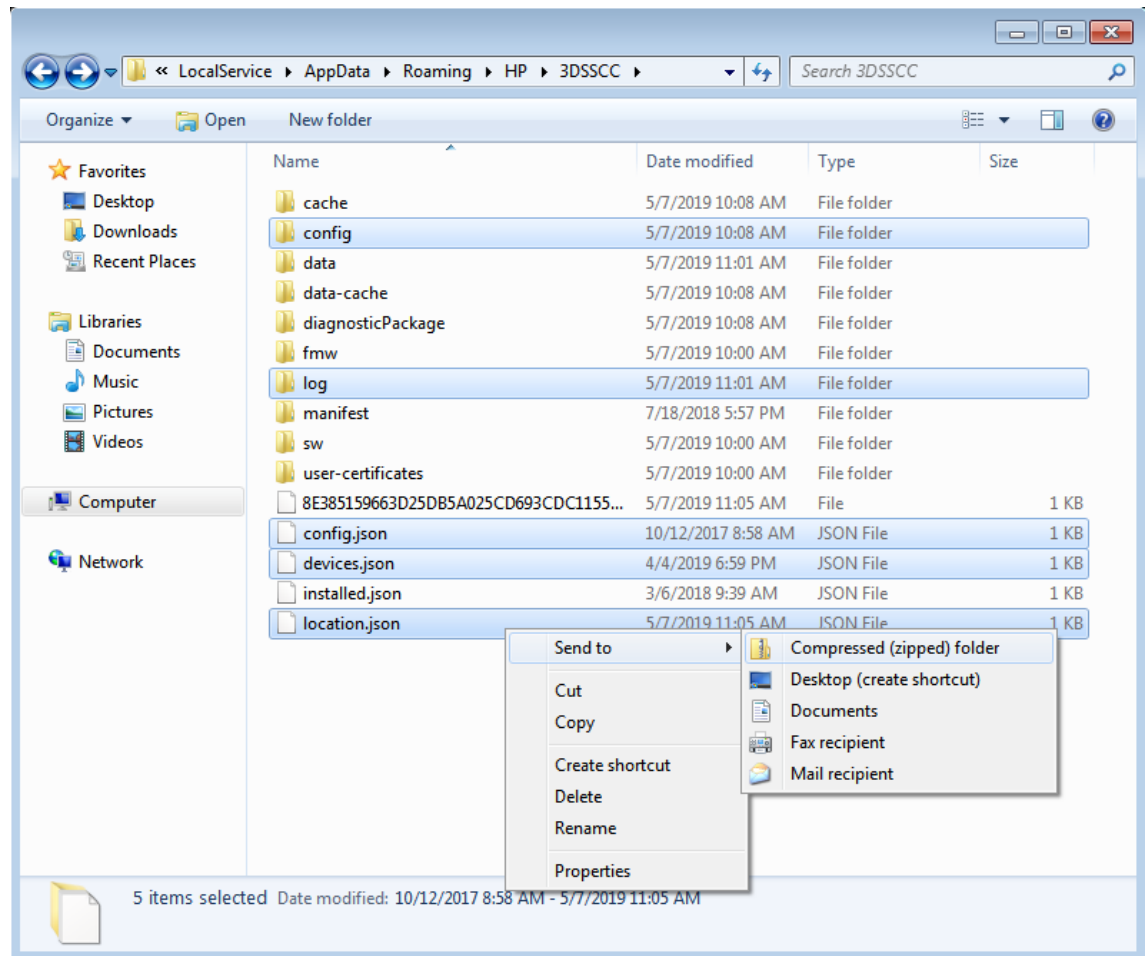
After this, the device should be connected to Command Center again.

Extract debugging information from the Command Center Server

Symptoms: In case of problems, extracting the debugging information from the Command Center Server can be helpful for the HP support team to find the cause of the problem.

Solution: Go to

C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\HP\
and create a zip file with the files config.json, devices.json, and location.json, and the folders log and config.



Check the **Access the Command Center application data folder** appendix section if you cannot access that application folder.

When you can access the directory, you can use the windows utility to compress a folder and generate a zip file. Consider that some files and folders may not be present on a recently installed Command Center.

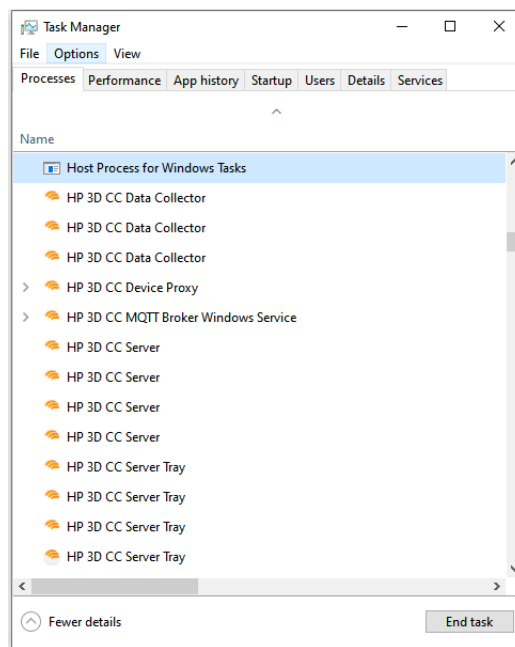
Check the **Accessing mosquito.log** file if you do not have permission to copy the file.

This .zip file will contain the needed information for debugging the Command Center.

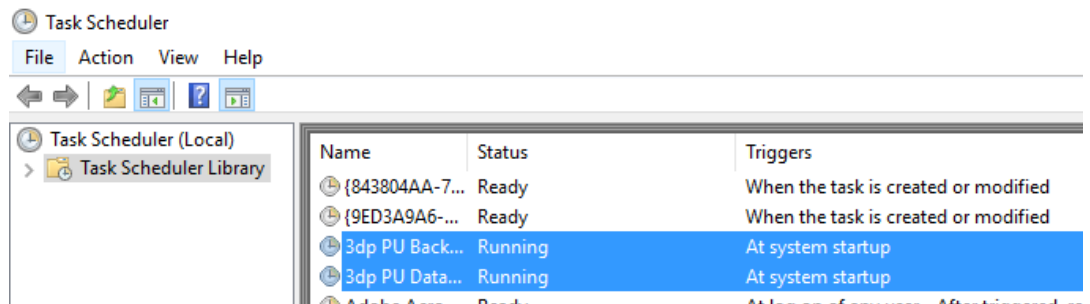
How to verify that all components are running

Go to the Windows Task Manager **Processes** tab and select show processes for all users if some processes are hidden. There should be one or multiple instances of HP 3D CC Client/Server, one or more of HP 3D CC Data Collector, as well as other services such as MQTT Broker or API Gateway services.

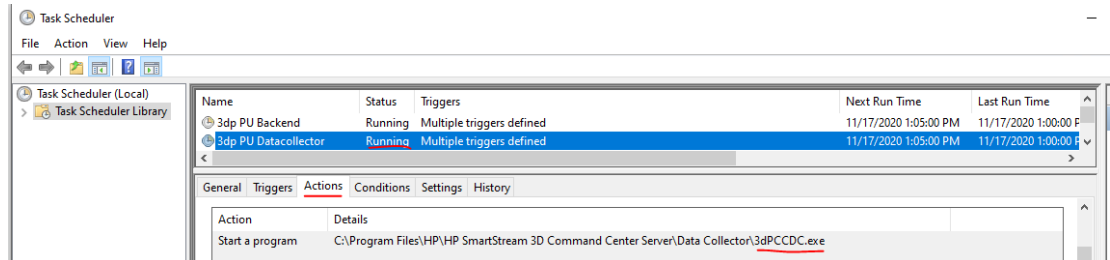
If any of the tasks are running, it means that it's working fine.



A second check is to open the Task Scheduler, where both “3dp PU Backend/Data Collector” tasks should be running. One controls the back-end (the server) and the other the Data Collector (to upload data to PrintOS). Once the Scheduled Task is selected, we can see the process that should run in the **Actions** tab, so, by going to the Task Manager as shown before, we can check if the underlying executable is running or not.



If both tasks are running, it means that it's working fine. It's very important to check this status any time the PC is restarted.

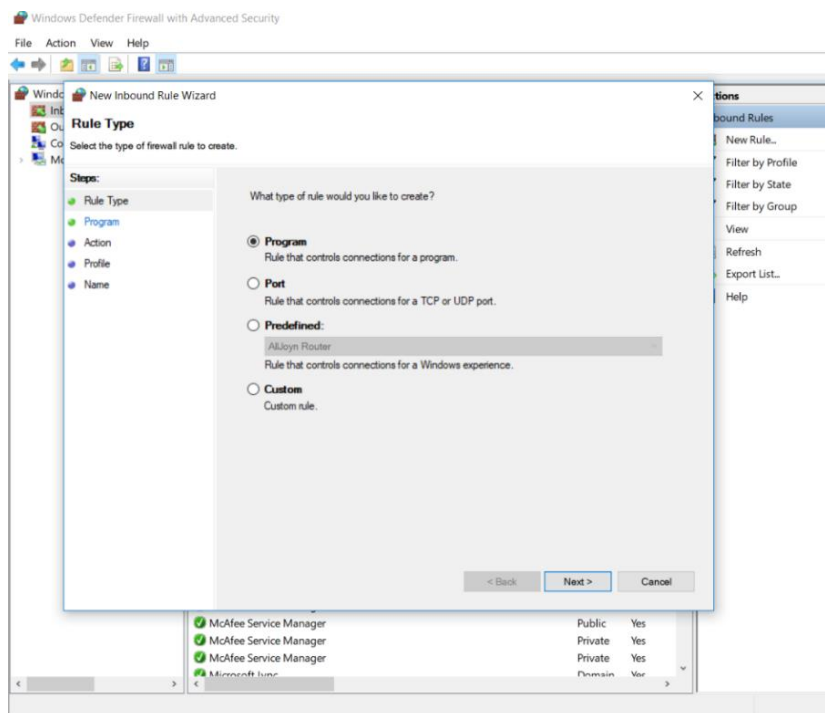


Check Internet connectivity to PrintOS, and between Command Center Server and Client

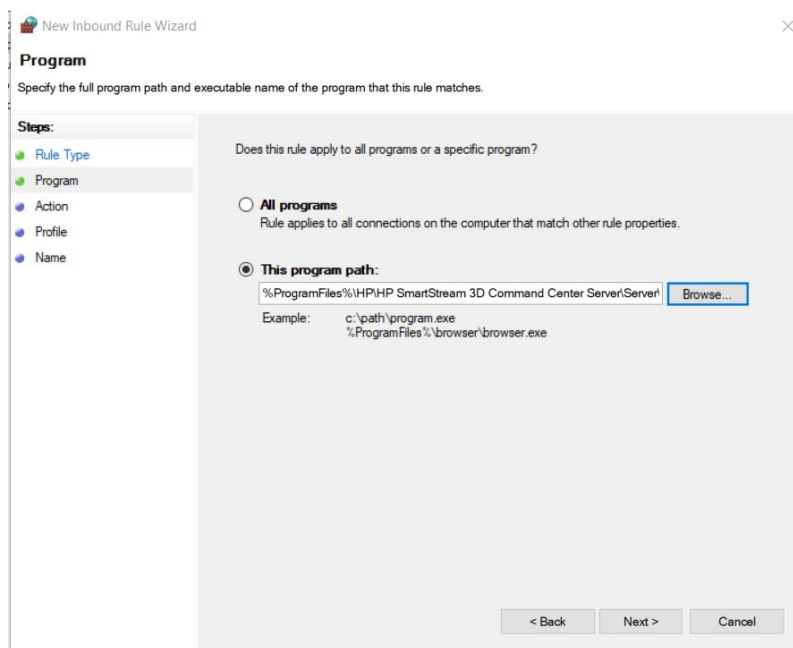
1. The computer where the Command Center Server is going to be installed must have Internet connectivity. Customers that heavily filter outgoing traffic should check that traffic to the HP Cloud endpoints is allowed (list below).
2. To check if HP Cloud endpoints are reachable, please follow the instructions in the section **Network diagnostics**.
3. The actual list of endpoints to allow in proxies/firewalls/... IT infrastructure the company uses to block outgoing traffic is given in the **IT Information** section.

To configure the firewall rule on the Command Center Server computer to allow Command Center Client connections follow these instructions: (If your company uses a third-party firewall on the computer contact your IT department).

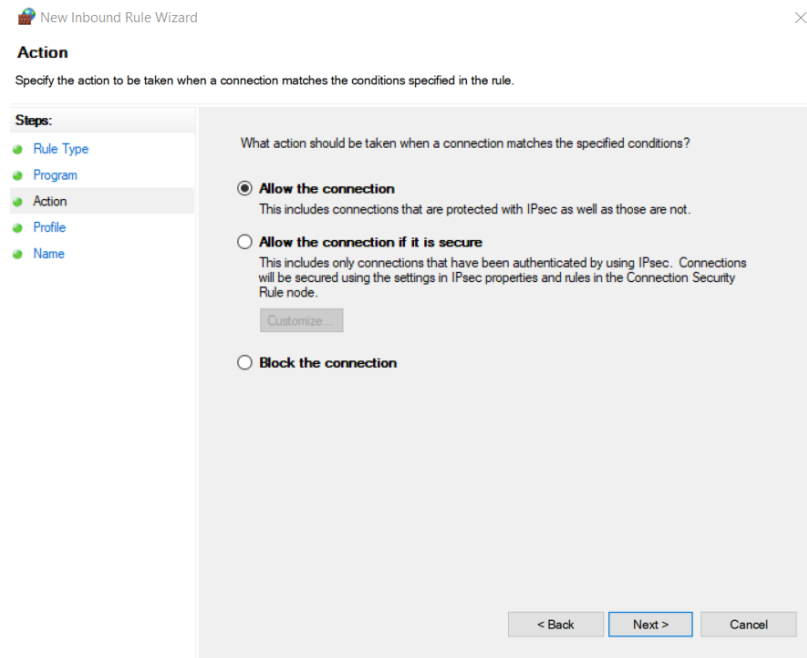
- a. Open Windows Defender firewall and select the option to add an inbound rule. Select **Program** and click **Next** (You can also select **Port** to specifically indicate the ports of the server and TCP protocol).



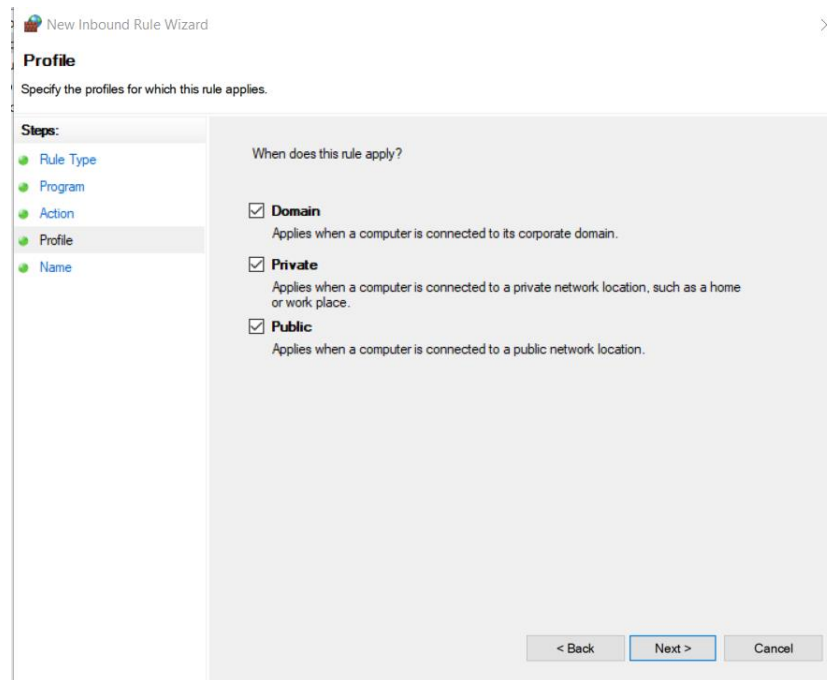
- b. Select the executable file of Command Center Server backend (usually located at C:\Program Files\HP\HP SmartStream 3D Command Center Server\Server\3dPCCServer.exe) and click **Next**.



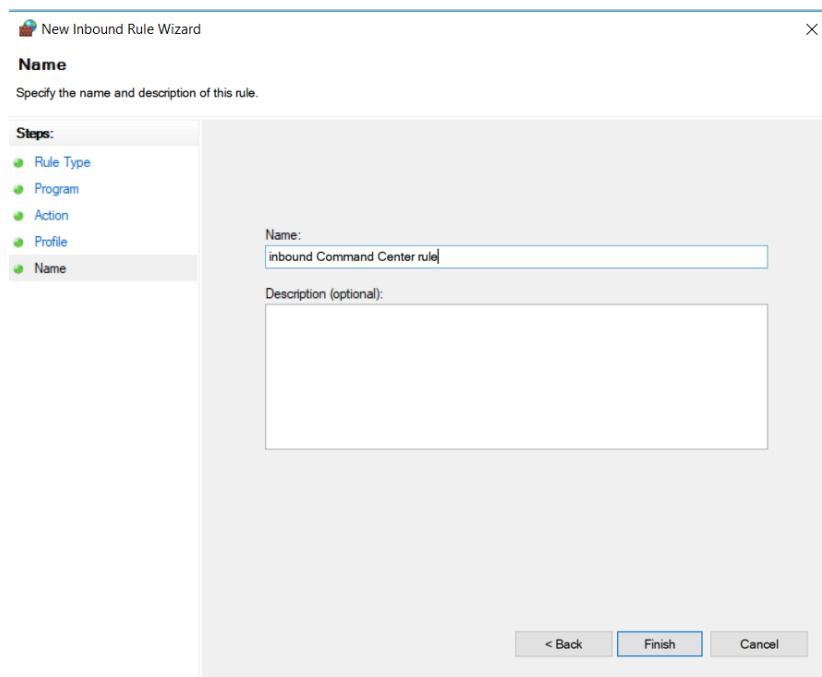
- c. Select **Allow the connection** and click **Next**.



d. Select all checkboxes.



e. Set a name for the rule just created and click **Finish**.



Command Center Server appear in the list, but it's disconnected

Symptom: When the Command Center Client starts, the “Network connectivity” screen appears and there’s a Command Center Server but there’s a “disconnected” message. This means the Command Center Client can “see” the Command Center Server, but cannot connect.

Solution: Click the small icon on the right to connect it.

Command Center Client is not able to log in to PrintOS

Symptom: When trying to log in to Command Center Client an error appears with the message “There was an error. Try again”.

Solution: Check your Internet connection. To log in to PrintOS with Command Center Client, an Internet connection with HP Cloud is required on both the Command Center Server and Command Center Client. The default browser must have connectivity as well.

If there are no connection errors with the cloud, check that you have accepted the message box mentioned in the section **Log in to PrintOS** once the login has been completed in your default browser. Consider that there is a timeout of 5 minutes to complete the login process in Command Center Client, and to accept the message box. Check the requirements in the **IT information** section.

If you have recently configured the proxy connection, check the section **Command Center Client is not able to log in to PrintOS after proxy configuration.**

Command Center Client is not able to connect to Command Center Server backend

Symptom: When the Command Center Client starts and the **Network connectivity → Server** tab does not find any server, and adding an IP and port for a well-known server backend does not work.

Solution: Consider that the Command Center Client must be in a network that can be routed to the network where the Command Center Server is located. You must change the priority of the network adapters on the Command Center Server to the desired one.

How you solve this will depend on the operating system used:

- For Windows 10:
<https://www.windowscentral.com/how-change-priority-order-network-adapters-windows-10>
- For Windows 7 or 8:
<https://support.microsoft.com/en-us/help/2526067>

Command Center Client is not able to log in to PrintOS after proxy configuration

Symptom: When the Command Center Client starts or after configuring proxy, PrintOS login is lost and/or you cannot log in again.

Solution: For proper operation of Command Center the proxy server must be able to route connections from the Command Center Client to the Command Center Server. The Command Center Server operating ports are in the range of 8443–8449 and 8080–8089, which must be open. If you have problems allowing connections through proxy, please ask your IT department for assistance.

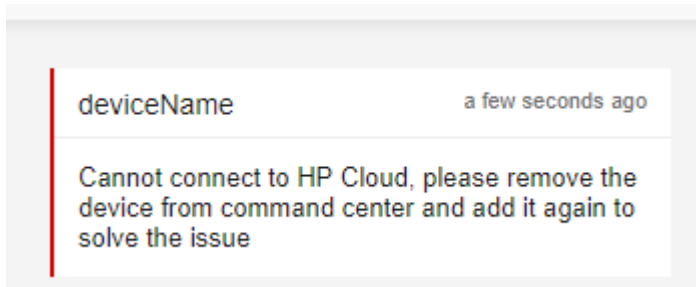
Configuring proxy settings on Windows 7

Symptom: When you try to configure a new proxy or update the configuration of current proxy settings on Windows 7, the Command Center doesn't work properly because it cannot connect to the Internet.

Solution: On Windows 7 machines, when you configure a proxy setting, you must reboot the operating system. The same action should be taken if you update information on the current proxy settings.

Device is not able to upload data to the HP Cloud

Symptom: The following alert is displayed:



Solution: It means that there is an error uploading device data to the HP Cloud and the Command Center is not able to fix it by itself. So, to fix the problem, it is necessary to remove the device and re-add it.

Problems connecting to a server

1. **Symptom:** A server is added to favorites and cannot be connected to from Command Center.

HOSTNAME/IP ADDRESS	PORT	VERSION	
15.	8080	2.3.3303 Incompatible	★ 🔗

Solution: This server is not compatible anymore, in order to connect to it upgrade Command Center Server to version 3.6 or later.

2. **Symptom:** A server is not auto-discovered.

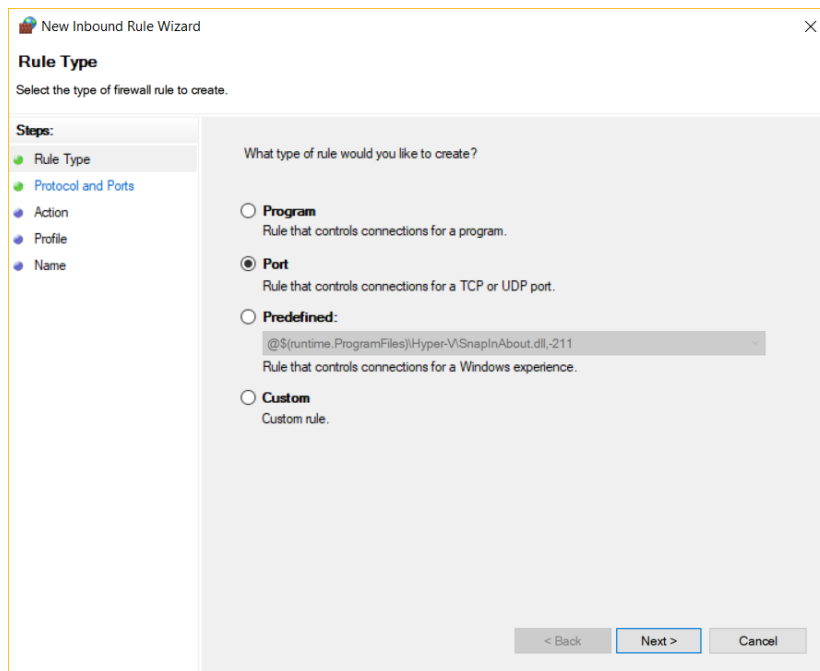
Solution: If your server version is earlier than 3.5, it is not compatible anymore, in order to connect to it upgrade Command Center Server to version 3.5 or later. If not, try to add it manually.

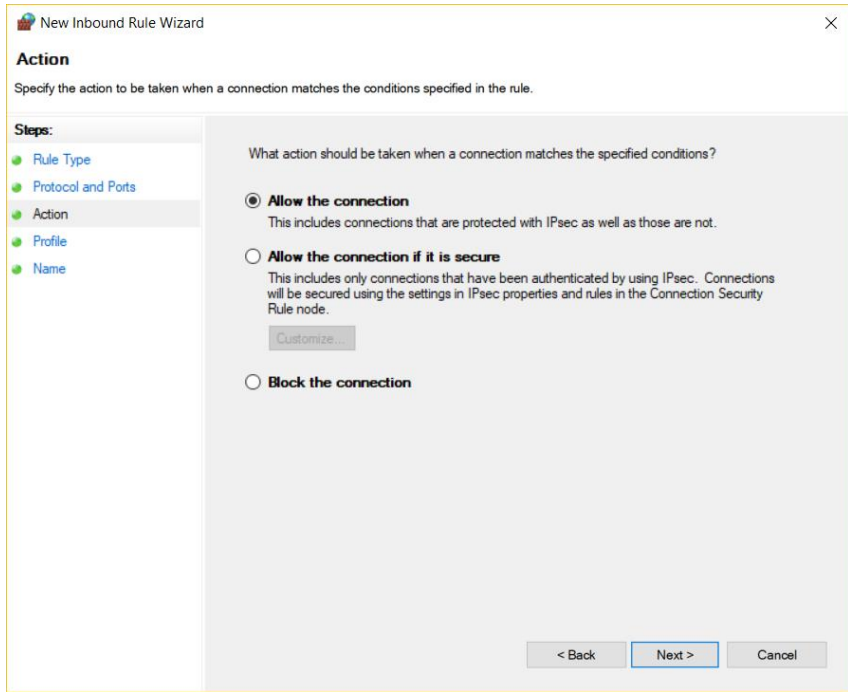
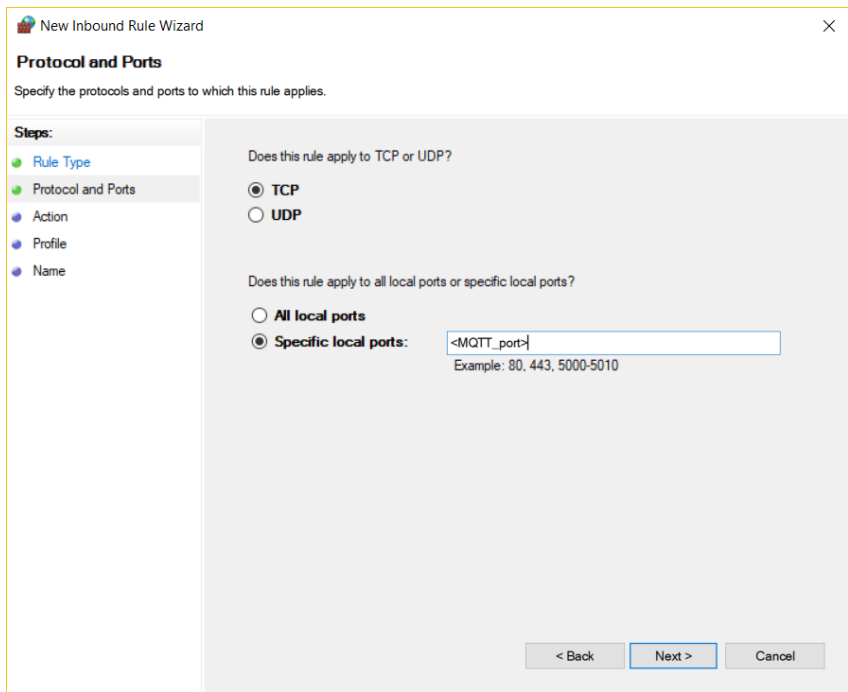
Problems connecting to the Command Center MQTT Broker

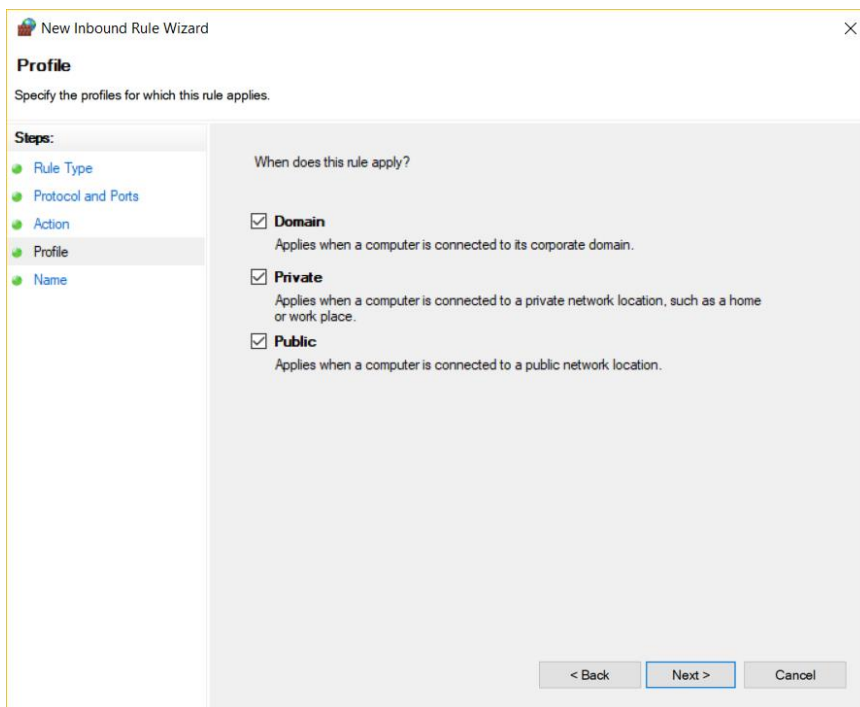
Symptom: The client is not receiving topic messages from the MQTT broker.

Solution: Make sure everything listed below is working:

1. The Command Center Server is using the correct port. Go to **Server installation** for more information.
2. The MQTT Broker service is running. Get Command Center Server / discovery to know which port MQTT is using:
GET https://<Server_IP>/discovery
3. The client connected to the MQTT Broker has received a connection notification message from **Device/Connectivity/MQTT** topic: *["timestamp":0, "context": 0, "payload":{"state": "Online"}]*
4. The client is registered to the topics of interest. For more information on how to register for the topics go to the section
5. **Connecting to Command Center MQTT** broker.
6. If everything above is working, the connection is probably blocked by the firewall. The solution is to add a new rule to the firewall to open the port that MQTT is using. To do so, go to **Windows Defender Firewall with Advanced Security** -> **Inbound Rules** -> **Add rule**.







Problems connecting to the Command Center Device API Gateway

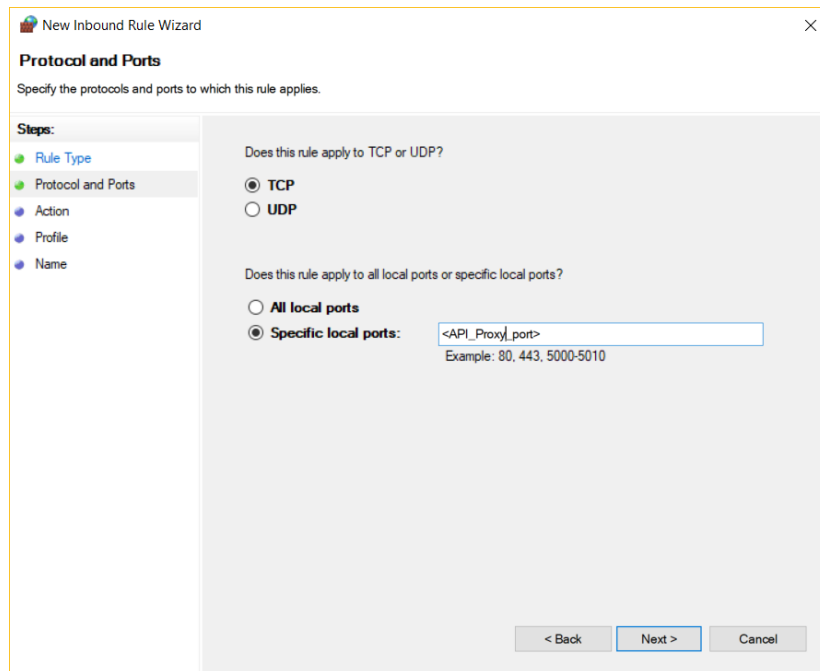
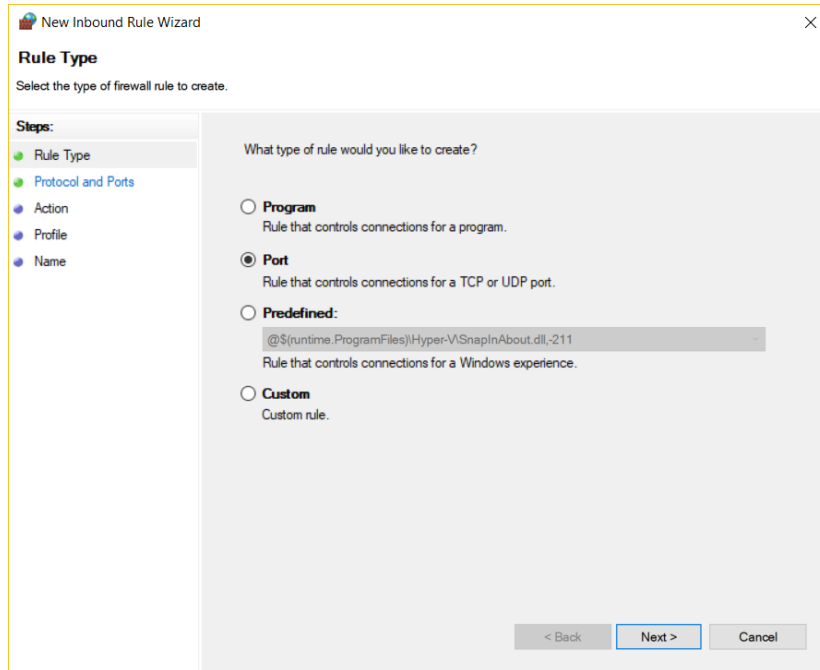
1. **Symptom:** The client receives a 401 Unauthorized response when doing a request to the API Gateway.

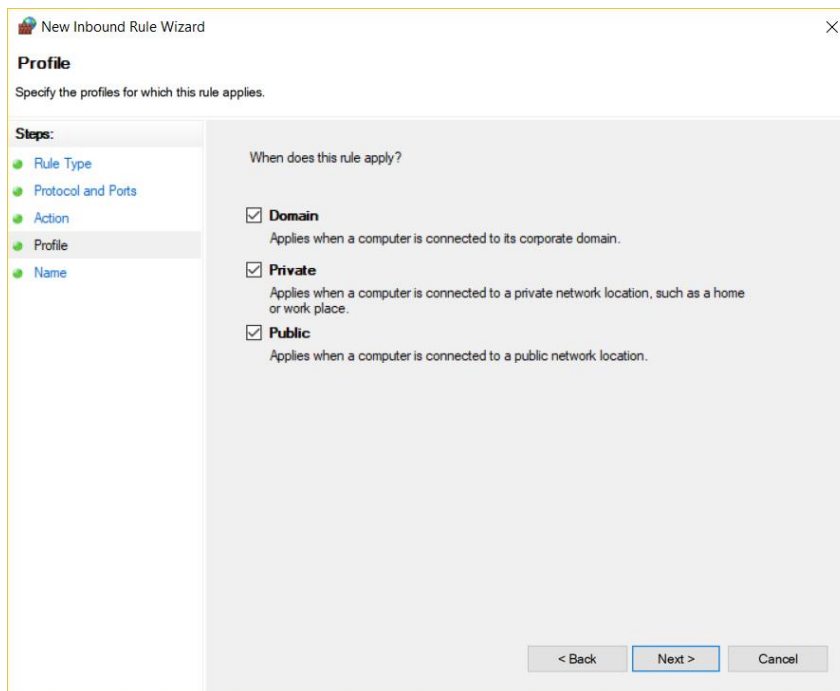
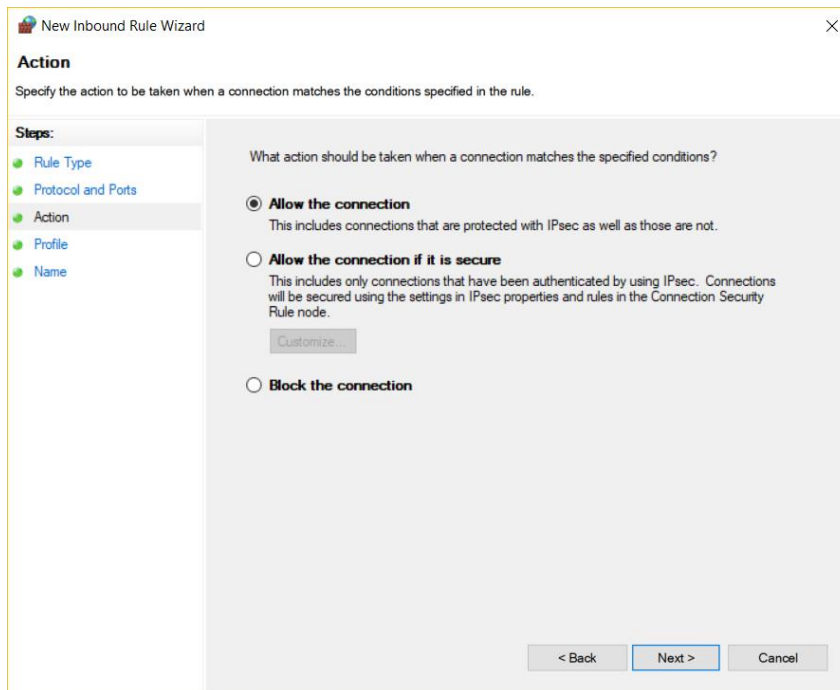
Solution: This problem is caused by an invalid token, so you will need to generate a new one, using the proper endpoint. This is explained in the guide you can find in the section **Connecting to the Command Center** .

2. **Symptom:** The client cannot see the Device API Gateway.

Solution: Add a rule to the firewall to allow connection to the port that Device API Gateway is using. Check the section **Connecting to the Command Center** for more information on how to check the Device API Gateway port.

To add a rule, go to **Windows Defender Firewall with Advanced Security** → **Inbound Rules** → **Add rule**.





Device Management or Add device button does not appear in Command Center Client

Note: To monitor or manage devices, you must be logged in to PrintOS with Command Center Client. Check the Command Center Client is connected to the Command Center Server correctly. If you have problems connecting to the Command Center Server, please check the section **Command Center Client is not able to connect to Command Center Server backend**.

Symptom: When the **Device Management** section is disabled or the **Add device** button does not appear in your Command Center Client.

Solution: If you are successfully logged in to PrintOS, and the **Add device** button does not appear, it means that your user is not an Administrator in any organization of the HP 3D family in PrintOS and you may need to contact your organization's PrintOS administrator to grant administrator permissions in your user account.

If you have problems logging in to PrintOS with Command Center Client, please check the section **Command Center Client is not able to log in to PrintOS**.

Remove device button does not appear in Command Center Client Device Management

Note: To monitor or manage devices, you must be logged in to PrintOS with Command Center Client. Check the Command Center Client is connected to the Command Center Server correctly. If you have problems connecting to the Command Center Server, please check the section **Command Center Client is not able to connect to Command Center Server backend**.

Symptom: When the **Remove device** button does not appear in your Command Center Client.

Solution: If you are successfully logged in to PrintOS, and the **Remove device** button does not appear, it means that your user is not an Administrator in any organization of the HP 3D family in PrintOS and you may need to contact your organization's PrintOS administrator to grant administrator permissions in your user account.

If you have problems logging in to PrintOS with Command Center Client, please check the section **Command Center Client is not able to log in to PrintOS**.

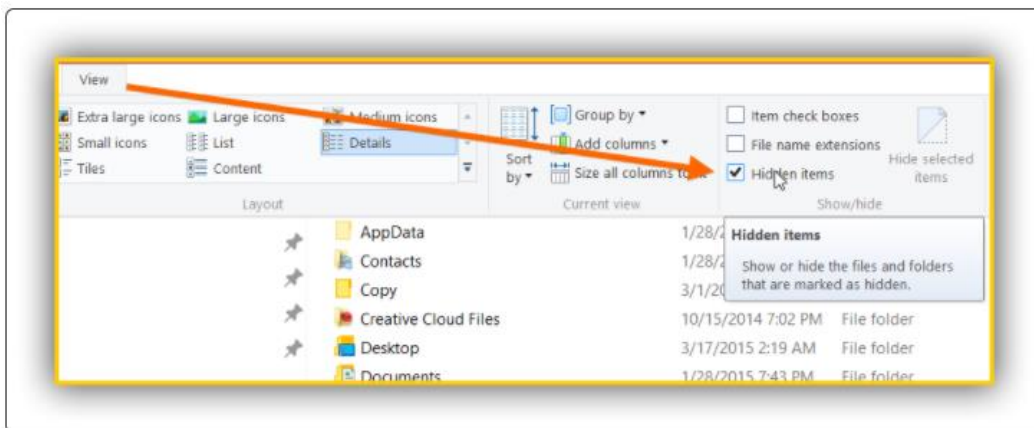
Appendix

Access the Command Center application data folder

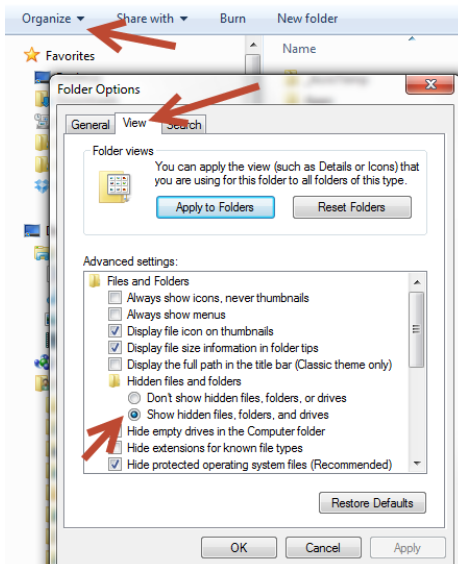
If you cannot see the AppData folder, it could be because it's hidden from view.

- For Windows 8 or 10:

Check by launching Windows Explorer and then click the **View** menu on the ribbon. Then ensure the option **Hidden items** is selected. It is important to close the Explorer and then reopen it after doing the change:



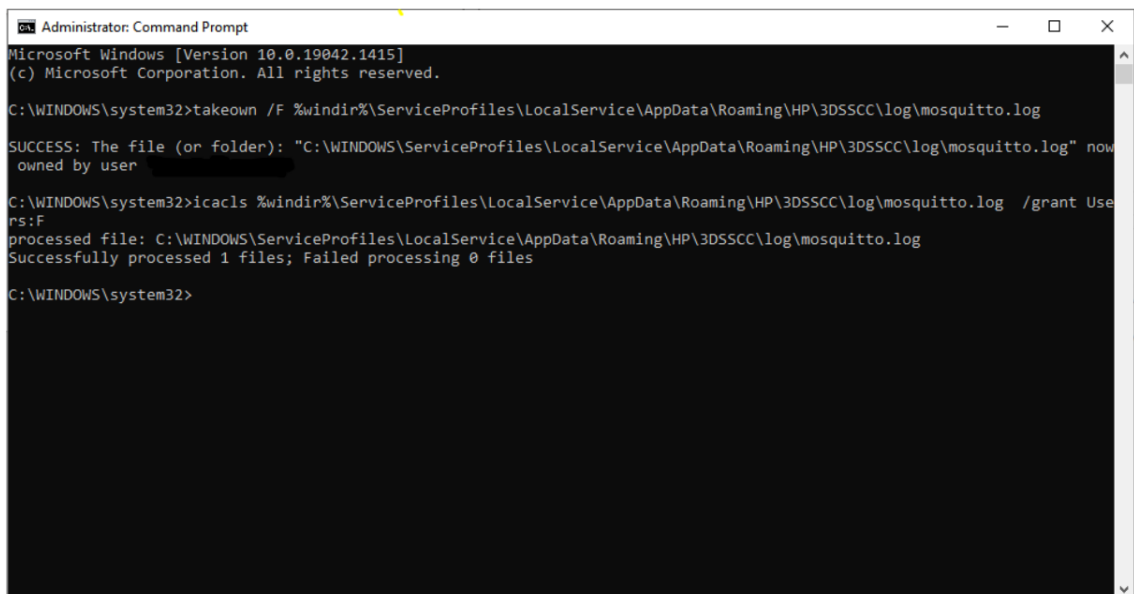
- For Windows 7:
 1. Go to Windows Explorer.
 2. Open the C: drive.
 3. Click **Organize** on the menu bar.
 4. Select the Folder and Search options.
 5. Select the **View** tab.
 6. Under **Files and Folders** → **Hidden files and folders**, select the option to **Show hidden files, folders, and drives**.
 7. Click **Ok**.



Accessing mosquito.log file

If you do not have permission to copy the file, open a Command Prompt as Administrator to grant access to your user. Write the following commands:

- `takeown /F`
`%windir%\ServiceProfiles\LocalService\AppData\Roaming\HP\3DSSCC\log\mosquito.log`
- `icacls`
`%windir%\ServiceProfiles\LocalService\AppData\Roaming\HP\3DSSCC\log\mosquito.log /grant Users:F`



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.1415]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>takeown /F %windir%\ServiceProfiles\LocalService\AppData\Roaming\HP\3DSSCC\log\mosquito.log
SUCCESS: The file (or folder): "C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\HP\3DSSCC\log\mosquito.log" now owned by user

C:\WINDOWS\system32>icacls %windir%\ServiceProfiles\LocalService\AppData\Roaming\HP\3DSSCC\log\mosquito.log /grant Users:F
processed file: C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\HP\3DSSCC\log\mosquito.log
Successfully processed 1 files; Failed processing 0 files

C:\WINDOWS\system32>
```

©Copyright 2022 HP Development Company, L.P. The information contained herein is subject to change without notice.

The information contained herein is provided for information purposes only. The only terms and conditions governing the sale of HP 3D printer solutions are those set forth in a written sales agreement. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty or additional binding terms and conditions. HP shall not be liable for technical or editorial errors or omissions contained herein and the information herein is subject to change without notice.