



User Manual

Product Version: v1.2 | Document Version: v1.2

Table of Contents

ABOUT THIS DOCUMENT	4
HOW IT WORKS.....	5
SYSTEM REQUIREMENT	5
INSTALL DEVICE MANAGER	6
RUN THE APP	6
LOG IN TO SERVER	7
WHEN BOTH THE CLIENT AND THE SERVER APPS ARE INSTALLED	7
WHEN ONLY THE CLIENT APP IS INSTALLED	9
DEVICE MANAGER CLIENT WORKSPACE	10
REMOTE CONNECTION.....	13
ADD DEVICE.....	13
DELETE DEVICE.....	15
ADD SITE	15
AUTHORIZE DEVICE	16
SET PASSWORD	16
ASSIGN IP ADDRESS.....	17
UPLOAD	18
<i>Upload Certificate (HTTPS)</i>	<i>18</i>
<i>Upload Certificate (IEEE 802.1x)</i>	<i>20</i>
<i>Upload Configuration File.....</i>	<i>21</i>
<i>Upload Firmware</i>	<i>22</i>
<i>Upload License.....</i>	<i>24</i>
<i>Upload Package</i>	<i>24</i>
QUICK SETUP.....	25
SET CONFIGURATION	26
CREATE TEMPLATE.....	26
IMPORT TEMPLATE	28
EXPORT DEVICE LIST OR DEBUG INFORMATION	29

REFRESH	29
ACCOUNT MANAGEMENT	30
VIVOTEK SERVICE MANAGEMENT	30
LOG OFF FROM SERVER.....	31

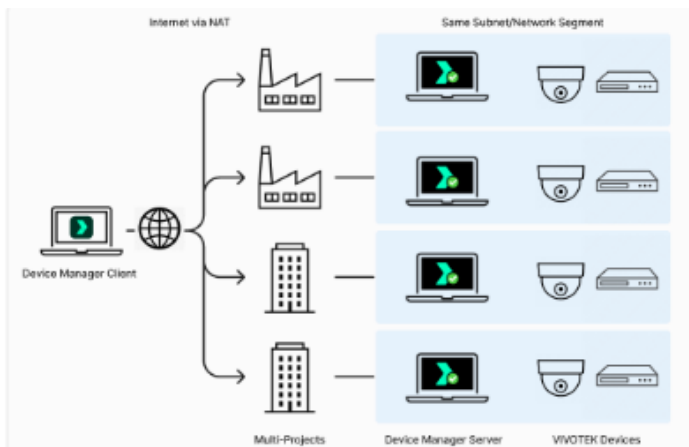
About this Document

Rev. 1.0: This document is written for Device Manager revision 1.0.0.0 or later.

Rev. 1.2: This document is written for Device Manager revision 1.2.0.0. or later.

How it works

The Device Manager is an installation and management tool that helps facilitate the configuration of multiple cameras via a client-server framework. Thus, camera management and maintenance can be done remotely by using the Device Manager client. Device Manager can also store all previously added cameras on a device list every time you open Device Manager and can automatically search the network for cameras, assign IP addresses, display connectivity, manage firmware/software upgrades, and collectively configure multiple cameras.



The Device Manager client can only login to one server at a time.

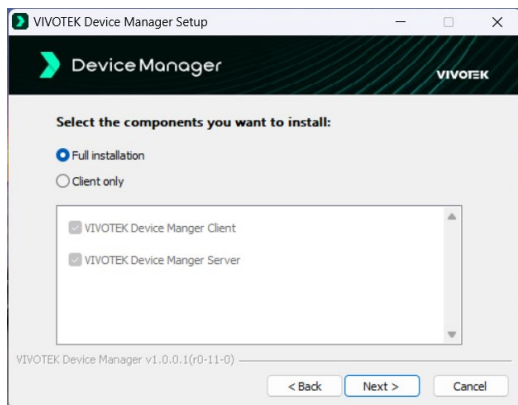
System Requirement

Operating System: Windows 10

CPU: 11th Generation Intel® Core™ i5 Desktop Processors

RAM: 16GB

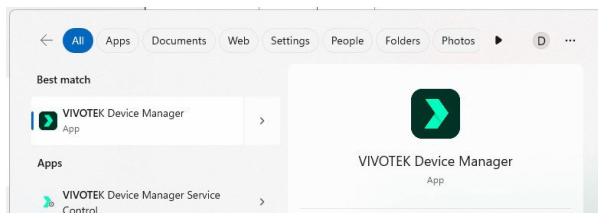
Install Device Manager



Device Manager has two components (apps). One is the client app (VIVOTEK Device Manager) and the other is the server app (VIVOTEK Device Manager Service Control). When installing Device Manager, you can select full installation (with both the client and the server apps) or the client only (with the client app only) depending on your requirements:

- On the server computer: You must select full installation.
- On the client computer: Select **Full installation** if the client computer will serve as both a client and a local server.
- On the client computer: Select **Client only** if the client computer will serve as a client only (no local server on the client computer).



Run the App



- To run the client app: Click windows (**Start**) > **VIVOTEK Device Manager**

- To run the server app (service): Click windows (**Start**) > **VIVOTEK Device Manager Service Control**



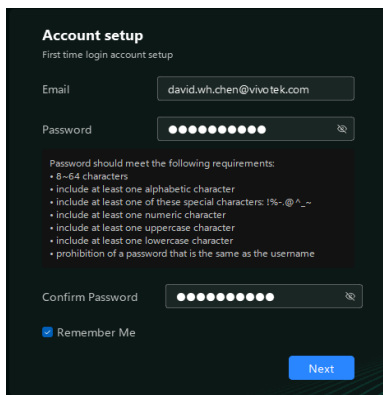
The server service (VIVOTEK Device Manager Service Control) is always running in the background after you install Device Manager. You can find the corresponding icon  and the right-click menu in the Windows notification area. (You may need to click the **Show hidden icons** arrow  to locate the server service.)

Log in to Server

When both the client and the server apps are installed

Run the client app (Device Manager) and follow the steps below:

1. Create an administrator (root) account (exclusively for use with Device Manager; a combination of email and password) for the local server, then click **Next**.



Account setup
First time login account setup

Email

Password

Password should meet the following requirements:


- 8~64 characters
- include at least one alphabetic character
- include at least one of these special characters: !%&@^_~
- include at least one numeric character
- include at least one uppercase character
- include at least one lowercase character
- prohibition of a password that is the same as the username


Confirm Password

☒ Remember Me


Next

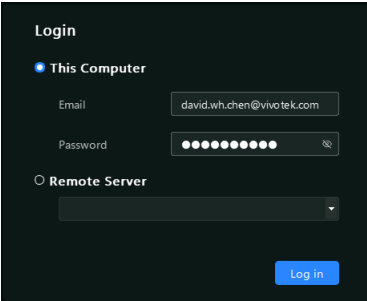
2. The account info you just entered displays under **This Computer** (local server) section. Now click **Log in** to open the Device Manager main screen.

To change the password for the local server, click  and select **Account Management**.

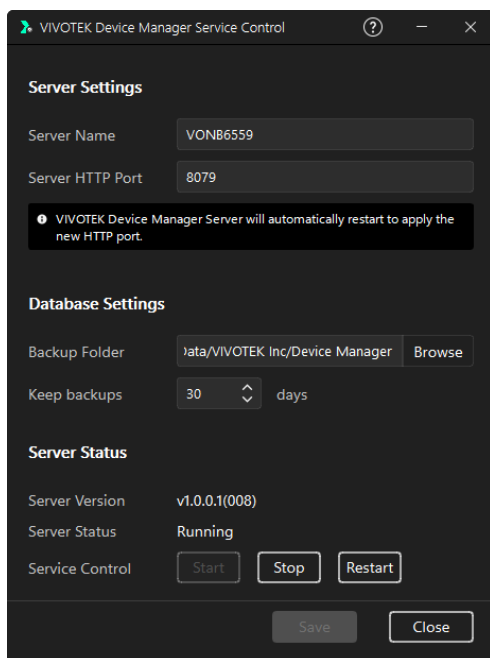
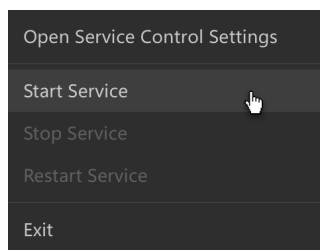
 If you have logged in to a server previously, the next time you run Device Manager, you will be directed to the login window directly (Account setup window will be skipped).

Service control settings of device manager:

1. In the Windows notification area, right-click the icon  and select **Open Service Control Settings** to open the Settings window.
2. Adjust settings as needed.
3. Click **Save**.
4. Decide how you want to run the service (Start/Stop/Restart).
5. Click **Close**.



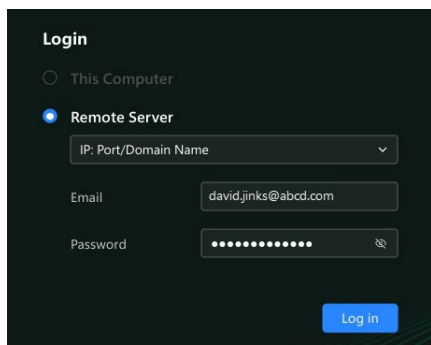
The screenshot shows a dark-themed login window titled "Login". It has two main sections: "This Computer" (selected with a blue dot) and "Remote Server" (unselected with a grey dot). Under "This Computer", there are fields for "Email" (containing "david.wh.chen@vivotek.com") and "Password" (represented by 10 dots). Under "Remote Server", there is a dropdown menu. A blue "Log in" button is at the bottom right.



When only the client app is installed

Run the client app and follow the steps below:

1. For the first time login, enter the login information — the administrator (root) account — for a remote server. If you previously connected to a remote server, select a server from the Remote Server drop-down list.
2. Click **Log in** to open the Device Manager main screen.

The image shows a dark-themed login window titled "Login". It has two radio buttons: "This Computer" (unselected) and "Remote Server" (selected). Below the "Remote Server" option is a dropdown menu labeled "IP: Port/Domain Name". Underneath the dropdown are two input fields: "Email" with the text "david.jinks@abcd.com" and "Password" with masked characters. A blue "Log in" button is located at the bottom right of the form.

Login

☐ This Computer

☒ **Remote Server**

IP: Port/Domain Name

Email david.jinks@abcd.com

Password

Log in

Device Manager Client Workspace

The Device Manager Client workspace is divided into four main sections: the Navigation Bar, the Main area, the Top Bar, and the Notification area. The following details the functions of each section:

- **Navigation Bar:** This allows users to switch between Device Management, System Logs, and System Settings main interfaces, enabling users to access the main functions of the Device Manager.
- **Main Area:** This varies based on the selected Navigation Bar content. For instance, in the Device Management section, users can access interfaces such as Remote Connection, Site Management, and Device List.
- **Top Bar:** This section provides settings for the logged-in account, version information, and links to the users manual, along with other relevant settings and information.
- **Notification Area:** This area provides real-time updates on system alarm information and the status of tasks executed by the users.

Navigation Bar **Top bar**

Remote connection Site

Status	Model	Host Name	IP	MAC	Firmware
Authorized	MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.234	0002D1ACE1EA	1.2302.39.01f
Authorized	FD9365-EHTV-v2	FD9365-EHTV-v2	10.42.1.241	0002D1A6E50D	1.2301.37.01e
Authorized	FD9391-EHTV-v2	FD9391-EHTV-v2	10.42.1.238	0002D1A6FE04	1.2301.37.01e
Authorized	MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.236	0002D1ACE1D8	1.2303.39.00a
Authorized	MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.232	02D07C6017A5	1.2303.39.00a
Unauthorized	FD9391-EHTV-v2	FD9391-EHTV-v2	10.42.1.235	0002D1A6FE1D	1.2302.37.01h
Authorized	MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.233	0002D1ACE1ED	1.2401.39.01a
Authorized	FD9365-EHTV-v2	FD9365-EHTV-v2	10.42.1.240	0002D1A6E51A	1.2202.37.00a
Authorized	MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.231	0002D1ABF187	1.2303.39.00a
Authorized	FD9365-EHTV-v2	FD9365-EHTV-v2	10.42.1.237	0002D1A6E517	1.2302.37.01h

Main area

Notification area

Date/Time	Source	User	Description
2024/05/07 08:59	Device	localhost	Server has been started
2024/05/07 12:54	Device	localhost	Server has been started
2024/05/08 07:29	Device	localhost	Server has been started
2024/05/08 12:48	Device	localhost	Server has been started

Below picture and table show the different functions in four sections:

Device Manager

Remote connection Site


Status	Model	Host Name	IP	MAC	Firmware
Authorized	MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.234	0002D1	1.2302.39.01f
Authorized	FD9365-EHTV-v2	FD9365-EHTV-v2	10.42.1.241	0002D1	1.2301.37.01e
Authorized	FD9391-EHTV-v2	FD9391-EHTV-v2	10.42.1.238	0002D1	1.2301.37.01e
Authorized	MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.236	0002D1	1.2303.39.00a
Authorized	MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.232	02D07C	1.2303.39.00a
Unauthorized	FD9391-EHTV-v2	FD9391-EHTV-v2	10.42.1.235	0002D1	1.2302.37.01h
Authorized	MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.233	0002D1	1.2401.39.01a
Authorized	FD9365-EHTV-v2	FD9365-EHTV-v2	10.42.1.240	0002D1	1.2202.37.00a
Authorized	MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.231	0002D1	1.2303.39.00a
Authorized	FD9365-EHTV-v2	FD9365-EHTV-v2	10.42.1.237	0002D1	1.2302.37.01h

Functions in four sections:



- 1. Remote connection
- 2. Site
- 3. Settings
- 4. Search
- 5. All
- 6. Alarm
- 7. Task
- 8. Status
- 9. Model
- 10. Host Name
- 11. IP
- 12. MAC
- 13. Firmware
- 14. HTTP
- 15. HTTPS Port
- 16. HTTPS
- 17. IEEE 802.1X
- 18. SD Card Status
- 19. SD Card Usage(%)
- 20. Date/Time
- 21. Power Frequency(Hz)
- 22. Audio
- 23. 24. Search
- 25. Search

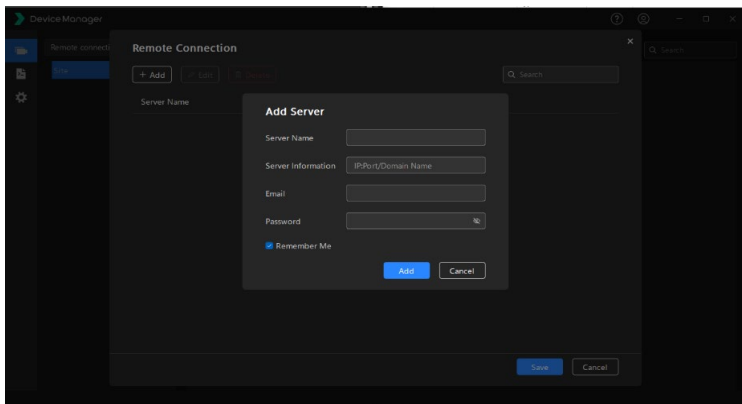
Sections	Item	Functions
Navigation Bar	1	Device management
	2	Log information
	3	General settings
Top Bar	4	User manual
	5	Account management
		VIVOTEK Service Management
		About
		Log off
Notification Area	6	Alarm
	7	Task
Main Area	8	Remote connection management
	9	Right-click menu
	10	Control bar
	11	Add device
	12	Delete device
	13	Authorize device
	14	Set password
	14	Assign IP
	15	Upload
	16	Quick setup
	17	Set configuration
	18	<i>Backup configuration (Coming Soon)</i>
	19	Restart device
	20	Restore device
	21	<i>Replace device (Coming Soon)</i>
	22	Export device list/debug info
	23	Refresh
	24	Search bar

Operation Tips

- Column on device list (ex. Status/Model):
 - (1) Click the column for sorting the content from A to Z.
 - (2) Right click the column to select what parameters to show or hide.
- Double-click a device in the device list to open the corresponding device management page in a browser.
- Click on  to expand the content of alarm or task.






Remote Connection

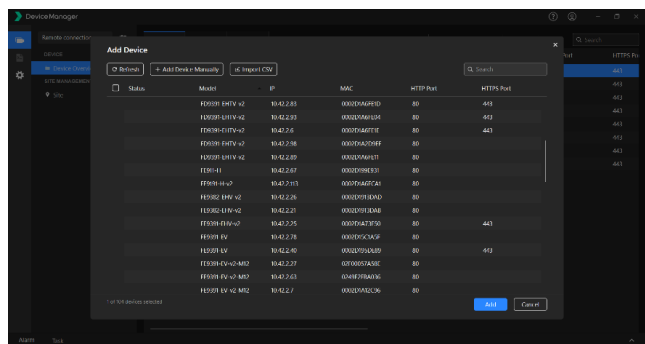
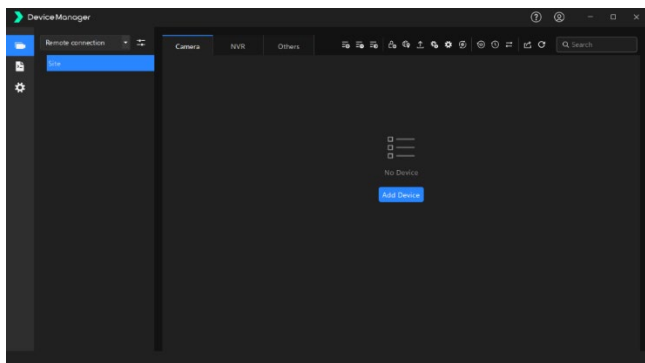
Because Device Manager uses a client-server structure, after the Device Manager client workspace appears, click  (remote connection management) to the right of the "Remote connection" drop-down list, and click  (under "Remote Connection") to set up a remote server that connects to the devices you want to manage.



Once you connect to a remote server, all devices connected to the server will populate in the device list on workspace.

Add Device

1. Users can click  or  (Add Device) in the workspace to add device.
2. Wait for Device Manager to check if it detects any camera on the same network segment where the connected server is located. If no camera is detected, the message "No Device" appears.
3. If the "No Device" message displays, you can choose one of the methods to add device:
 - (1) Click  to manually enter an IP range or specific IP information of device.
 - (2) Click  to import a Comma Separated Values (CSV) file containing device information to add devices.
4. Once users select the device wants to add, click  and wait for the detected camera list to populate.



Once the device is added, there will be different status of device showed in the device list with different situation, below table describes the definition of device's status.

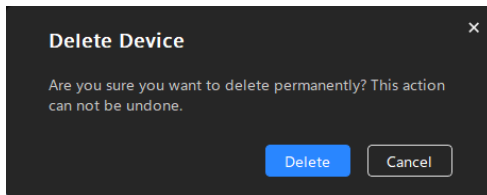
Status	Definition
Authorized	The device has been authenticated with the correct credentials. The device can perform all the buttons in the control bar.
Unauthorized	The device has not been authenticated with the correct credentials. The device can only perform authorized device button in control bar.
Unreachable	The device cannot be connected and cannot perform any button in control bar.
Account Blocked	Cameras with firmware version 2204 or later support an account block mechanism to comply with IEC-62443. If multiple failed login attempts occur within a short period, the camera will temporarily ban the originating IP address.

Invalid Password	The wrong credentials was entered. The device can only perform authorized device button in control bar.
Set Password	If a device is a newly installed or reset device, you can set up a password for better protection. The device can only perform the set password button in control bar.
Maintaining	The device is undergoing maintenance and cannot perform any button in control bar.

Delete Device

If you want to delete added devices from device list, use Ctrl or Shift key to select the devices you want to delete. Then click  (Delete Device). The following dialog box will appear, asking you to confirm the operation.

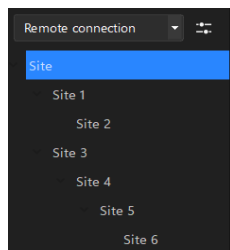
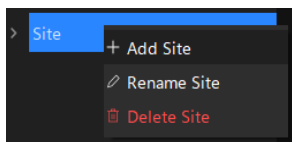
Note that, if you delete the device in one of the sites, the device will be deleted from the site only and will remains in the device overview, so if you want to delete the device permanently, please delete the device in device overview.




Add Site

After you create a remote server or add devices, by default, all detected devices will be listed under the Device Overview, you can start adding sites. In Device Manager, a customer site helps you organize devices more efficiently. You can drag to copy device(s) to any site you create. Just treat a site as a place where your devices are located.

To add a site, right-click the default site under the Remote connection drop-down list and select **Add Site** (maximum 4 layers of sites can be added). Then, use Ctrl or Shift key to select and drag devices to the site you want. (The Device Overview will still contain all the detected devices.)




Authorize Device

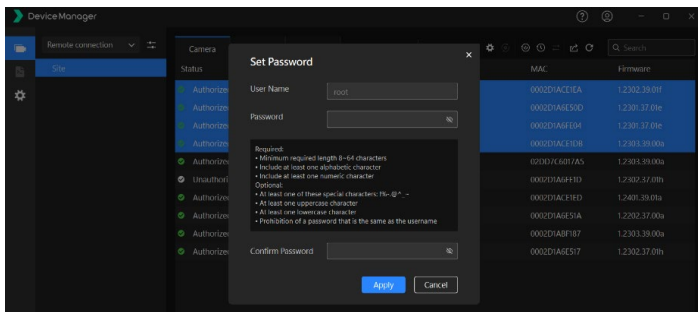
For devices protected by preset passwords, click to select them, then click  (Authorize Device button). This operation authorizes access to the devices for further configuration. Note that if you are without authorization, you will be prompted for a password whenever you want to configure a device.

Once a device is authorized, under the Status column the "Authorized" message will appear.

Set Password

When your device requires setting up a username and password for authentication during the initial setup phase, or if you want to update the authentication password for your device, you can use the "set password" feature to change the password.

Select the device that status is set password or authorized and click  to setup the new password for device.

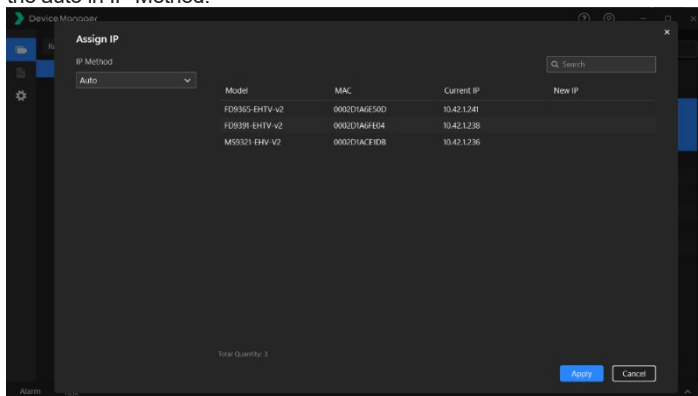


Assign IP Address

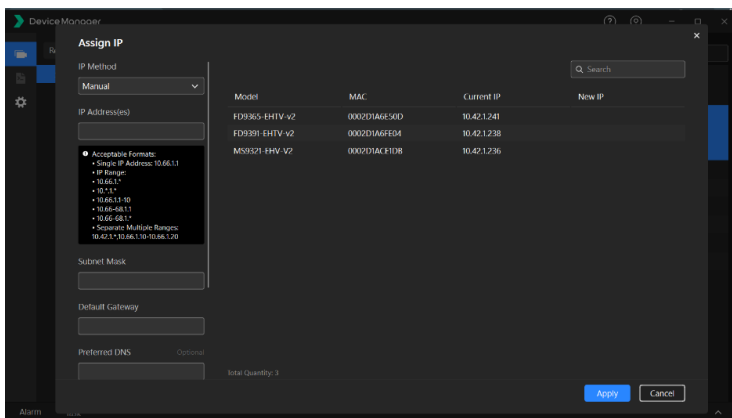
When you want to assign a range of fixed IPs to multiple cameras or random IPs assigned by DHCP server, you can use the assign IP feature.

Select the authorized devices and click  (Assign IP Address button) to assign IP addresses to one or multiple devices.

- If you want that IPs can be obtained automatically from a DHCP server, select the auto in IP Method.



- if you want that IPs can be assigned manually with an IP address range, select the manual in IP method.



Upload

During the maintenance of VIVOTEK devices, it is necessary to update the device firmware, certificates, license, configuration files and packages. Using the Device Manager's upload feature, users can batch update these components to ensure the devices are always running the latest and most stable versions.

Select the authorized device in device list and click  in the control bar to upload.

Upload Certificate (HTTPS)

1. Users can select to upload HTTPS certificate in upload certificate.
2. Select **HTTP & HTTPS** or **HTTPS only** as the connection option.
3. If needed, enter the value of HTTPS port.
4. Select one from the following three options:
 1. **Generate self-signed certificates:** Selects this if you want to use self-signed certificates created, issued and signed by VIVOTEK.
 2. **Create certificate request and install:** This method requires creating a certificate request on each camera's web interface and using each CSR in the PEM format for applying and generating certificate file. Select this if you have certificate files ready. Note that the file name should contain the MAC address of the target camera(00AABBCCDDEE or 00-AA-BB-CC-DD-EE).
 3. **Upload certificate and private keys:** Select this if you have both certificate and private key files ready. Note that the file name should

contain the MAC address of the target camera (00AABBCCDDEE or 00-AA-BB-CC-DD-EE).

5. Users can monitor the process in task and check the results after the task is finished.

Upload Certificate - HTTPS

Mode: HTTP & HTTPS

HTTPS Port: 443

Method: Generate self-signed certificate

Country: TW

State or province: Asia

Locality: Asia

Organization: VIVOTEK Inc.

Model	Host Name	IP	MAC
FD9387-EHTV-V3	FD9387-EHTV-V3	10.66.104.112	0002D1ACC86D
FE9192-H	FE9192-H	10.66.104.136	0002D198F1D2
IB9387-EHTV-V3	IB9387-EHTV-V3	10.66.104.111	0002D1AC8D38
MS9321-EHV-V2	MS9321-EHV-V2	10.66.104.85	0002D1913DAB
SD9384-EHL	SD9384-EHL	10.66.104.127	0002D196AEBF
IB9389-EHTV-v3	IB9389-EHTV-v3	10.66.104.108	0002D1A6FE1E

Total Quantity: 6

Apply Cancel

If HTTP certificate upload fails, one of the following messages may appear. Please find a suitable solution to solve the indicated problem.

1. **Mismatching private key and certificate:** *.crt and *.key do not match.
2. **Invalid file or public key:** The upload file is in the wrong format or the public key has problems.
3. **Mismatching status:** The selected camera has incorrect status. Ensure you have already created a certificate request on each camera's web interface and used the latest CSR in the PEM format for applying and generating the certificate file via uploading certificates request and installation.
4. **Failed to connect to device:** The process of uploading files to the camera was interrupted because of an unstable network environment.
5. **Device response timeout:** Possible causes may be that the file upload time exceeded the timeout, an unstable network environment or other abnormality occurred.
6. **Unsupported method:** The old camera firmware does not support the method of uploading certificates and private keys.
7. **File missing or failed to match file:** Possible reasons for the issue could be that the number of users-selected files is fewer than the number of cameras to

be updated, or that some file names do not contain the MAC address.

Upload Certificate (IEEE 802.1X)

For all selected authorized cameras, you can upload their IEEE 802.1X authentication files all at once:

1. Users can select to upload IEEE 802.1X in upload certificate.
2. Select EAP-PEAP or EAP-TLS as the EAP mode and its corresponding certificate files:
 - (1) **EAP-PEAP:** based on server-side certificate authentication.
 - (2) **EAP-TLS:** based on client certificate authentication. Note that the file name should contain the MAC address of the target camera(00AABBCCDDEE or 00-AA-BB-CC-DD-EE).

Model	Host Name	IP	MAC
FD9387-EHTV-V3	FD9387-EHTV-V3	10.66.104.112	0002D1ACC86D
FE9192-H	FE9192-H	10.66.104.136	0002D198F1D2
IB9387-EHTV-V3	IB9387-EHTV-V3	10.66.104.111	0002D1ACB038
MS9321-EHV-V2	MS9321-EHV-V2	10.66.104.85	0002D1913DA8
SD9384-EHL	SD9384-EHL	10.66.104.127	0002D196AEBF
IB9389-EHTV-v3	IB9389-EHTV-v3	10.66.104.108	0002D1A6FE1E

If IEEE 802.1X certificate upload fails, one of the following messages may appear. Please find a suitable solution to solve the indicated problem.

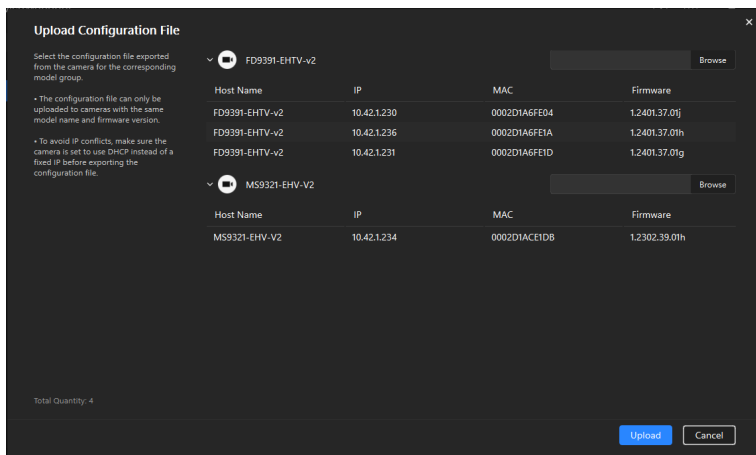
1. **Failed to connect to device:** The process of uploading files to the camera was interrupted because of an unstable network environment.
2. **Device response timeout:** Possible causes may be that the file upload time exceeded the timeout, an unstable network environment or other abnormality occurred.
3. **File missing or failed to match file:** Possible reasons for the issue could be that the number of users-selected files is fewer than the number of cameras to

be updated, or that some file names do not contain the MAC address.

Upload Configuration File

Users can upload the configuration files of a particular camera and apply to all other cameras of the same model.

1. Users can export the configuration file first via camera web.
2. Select a configuration file for the selected device on device list and click upload.



The following status of the configuration updating progress:

1. **File is uploading:** Device manager is uploading the file to the camera. Note that the process may take longer in a limited network environment.
2. **Camera is reconnecting:** The camera finishes updating configuration and starts rebooting.

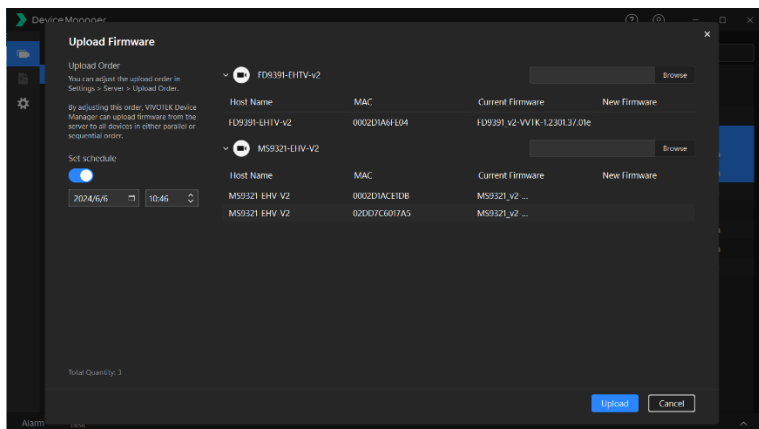
If upload fails, one of the following messages may appear. Please find a suitable solution to solve the indicated problem.

1. **Invalid file for this model group:** The configuration file may not correspond to the camera model or is incompatible.
2. **File upload timeout:** The upload process took longer than the expected or specified time.
3. **Failed to connect to device:** The upload process was interrupted because of unstable network environment.

4. **Device response time out or IP changed after rebooting:** cause by update time exceeded the timeout, the camera IP address change after update or other abnormality occurred.

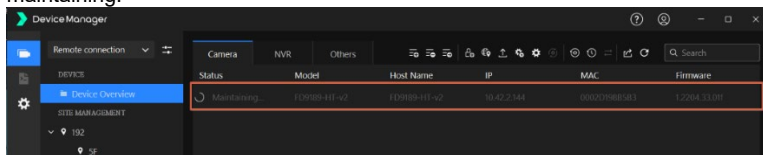
Upload Firmware

1. Users can adjust the upload order in setting, which can upload multiple cameras in either parallel or sequential order.
2. Users can toggle on set schedule to start the upload task in specific time.

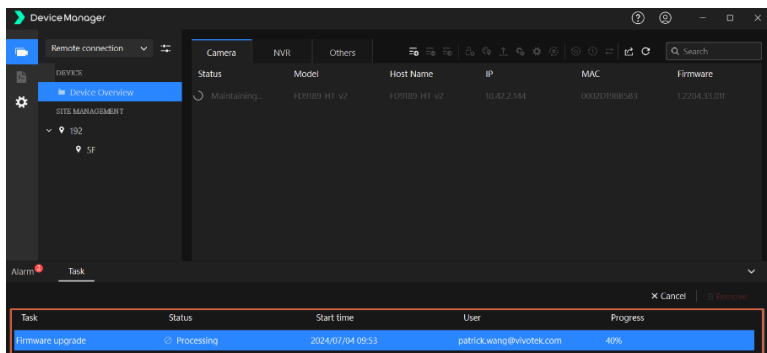


Select a firmware/software file for the selected device on device list

3. While uploading firmware, users can see the status of device turn into maintaining.



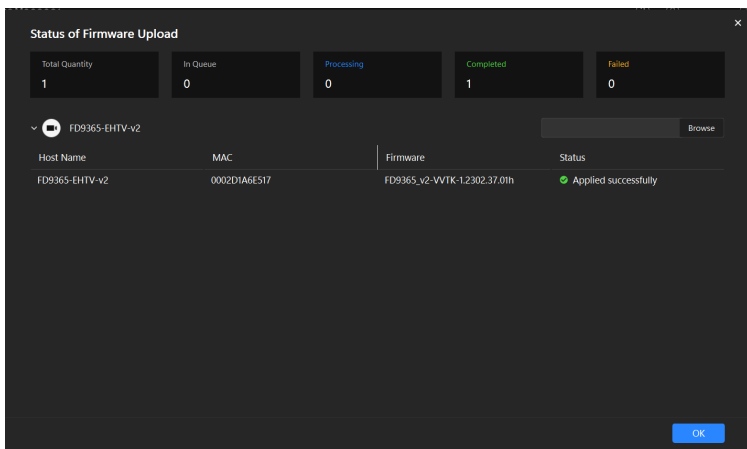
4. Users can also click the task to check the current progress



The following three status show the updating progress of firmware.

1. File is uploading
2. Camera is updating
3. Camera is reconnecting

Once the task is finished, users can double click the task to see in detail.



If firmware update fails, one of the following messages may appear. Please find a suitable solution to solve the indicated problems.

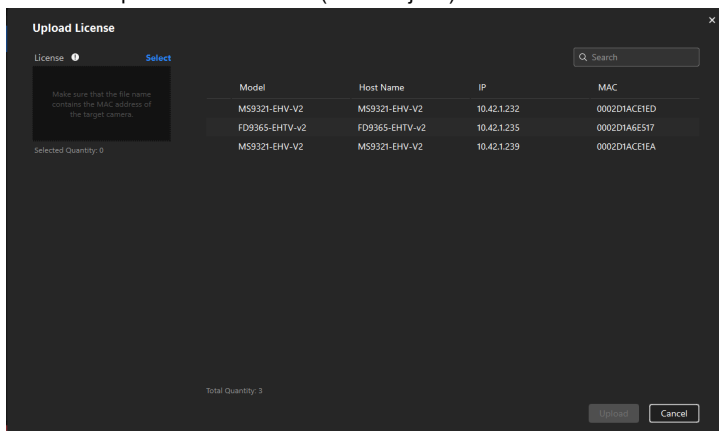
1. **Invalid file for this model group:** The firmware may not correspond to the camera model or is incompatible.
2. **File upload timeout:** The upload process took longer than the

expected/specified time. You can adjust the upload order in settings.

3. **Failed to connect to device:** The upload process was interrupted because of unstable network connection.
4. **Device response timeout or IP changed after rebooting:** Possible causes may include the update time exceeding the timeout, inability to detect if the update was successful due to IP address change, or other abnormalities.

Upload License

1. Users can upload the license file (*.txt or *.json) to device.



2. Users need to make sure the file name contains the MAC address of the target camera.
3. Select license files for the selected device on device list. If the file name of license file is not matched for selected devices, then there will be red hint show on the list.

	Model	Host Name	IP	MAC
❗	MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.232	0002D1ACE1ED
❗	FD9365-EHTV-v2	FD9365-EHTV-v2	10.42.1.235	0002D1A6E517
❗	MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.239	0002D1ACE1EA


Upload Package

Users can upload the VADP package to device.

1. Users can choose to upload the package to SD card if available for device.


2. Select the package file for selected devices on device list.

Upload Package

 CC9160-H

Model	Host Name	IP	MAC
CC9160-H	CC9160-H	10.42.2.98	0002D19B534F

☐ Save to SD Card


 MS9321-EHV-V2

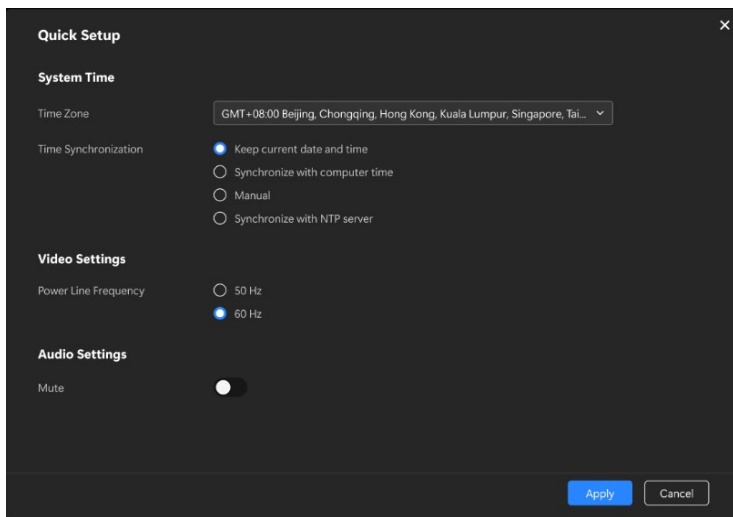
Model	Host Name	IP	MAC
MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.238	0002D1ABF187
MS9321-EHV-V2	MS9321-EHV-V2	10.42.1.232	0002D1ACE1ED

Total Quantity: 3

Quick Setup

Device Manager offers a Quick Setup feature that allows users to quickly configure the basic settings of their cameras. This enables users to rapidly deploy cameras to their sites.

Select the authorized devices and click on  to enable the quick setup. Users can setup system time, video settings or audio settings and click apply.



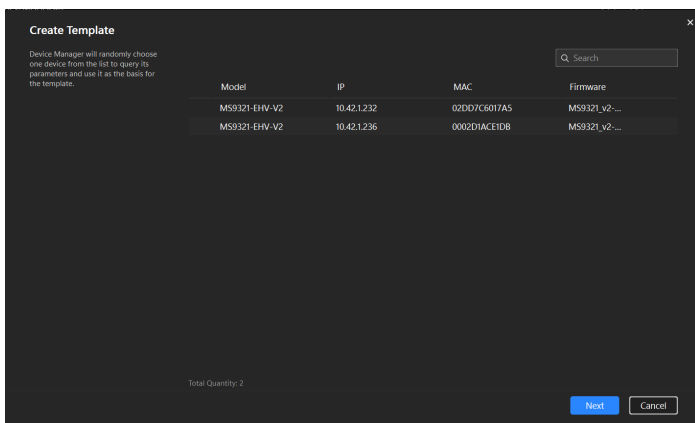
Set Configuration

The Set Configuration feature helps users to batch adjust camera settings or import previous configuration files to the cameras. However, please note that this feature is only available for devices of the same model and firmware version.

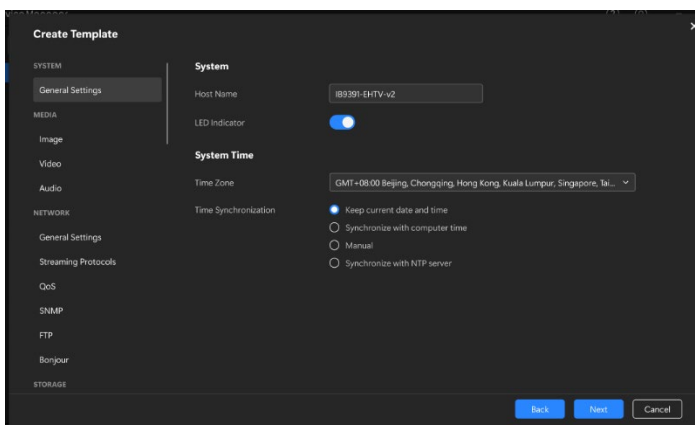
Select the authorized devices and click on  to select **Create Template** or **Import Template**.

Create Template

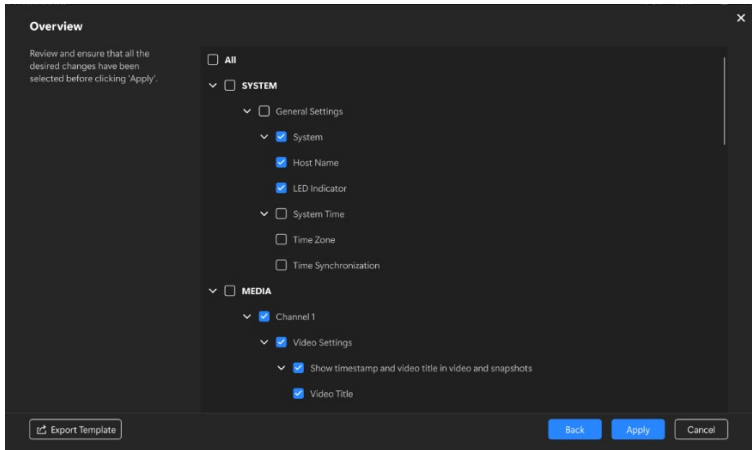
1. Users can check the device and firmware version.



2. Configure the settings and then click Next.



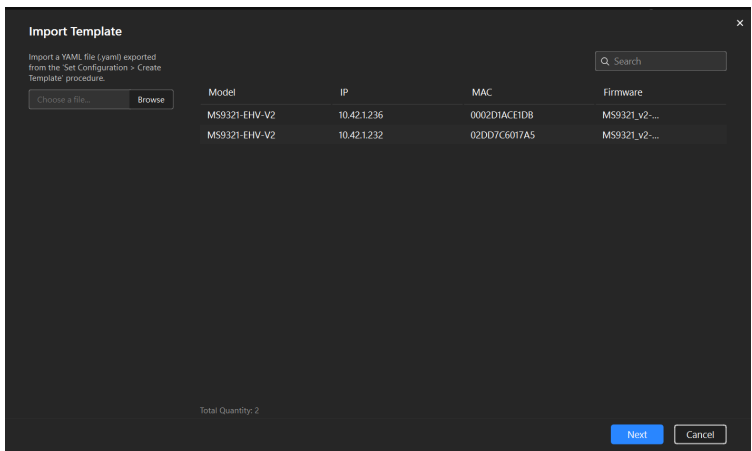
3. Review and select the modified settings that want to apply, then click Apply. Users can also export this setting as a template for reference.



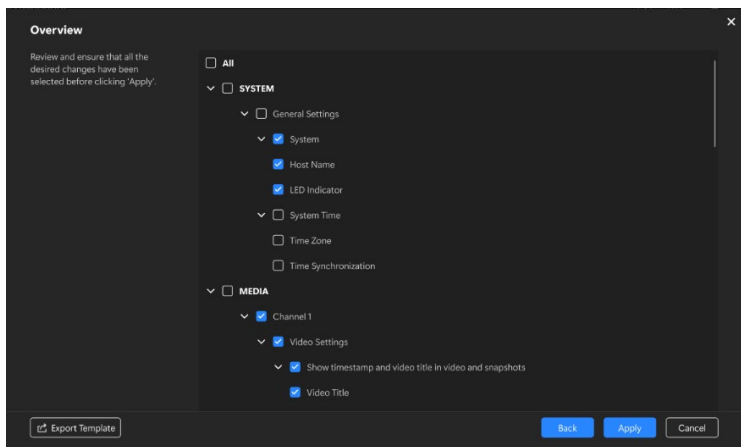
- Users can monitor the process in task and check the results after the task is finished.

Import Template

- Users can upload a configuration template and click Next.




- Review and select the modified settings that want to apply, then click Apply. Users can also export this setting as a template for reference.



3. Users can monitor the process in task and check the results after the task is finished.


Export Device List or Debug Information

Users can use the Export Device List/Debug feature to export the established device list for project maintenance purposes. Additionally, users can export debug information for problematic cameras to provide further analysis by technical support.

Select the authorized devices and click  (Export Device List button) to see two options:

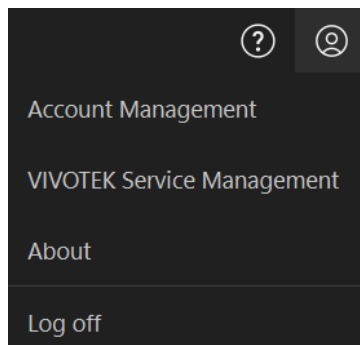
- **Device list** contains information of selected cameras. This list is especially useful if your deployment includes cameras residing in different subnets.
- **Debug info** contains log history and configuration file that facilitate problem solving if you need to contact VIVOTEK's technical support. VCA (Video Content Analysis) Package information is also included.

Refresh


Click  (Refresh button) if you want to let Device Manager retrieve latest device information again.

Account Management

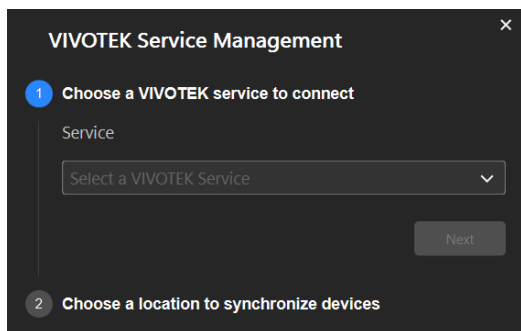
For change the account password, click  and select **Account Management**.

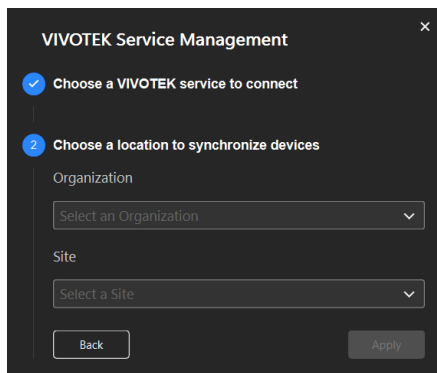


VIVOTEK Service Management

To enable device monitoring and remote access, click  and select **VIVOTEK Service Management**.


Follow the enabling process to select a VIVOTEK service, enter the corresponding credentials, and choose a customer and site to synchronize devices and enjoy the service.





The screenshot shows a dark-themed dialog box titled "VIVOTEK Service Management" with a close button (X) in the top right corner. The dialog contains two steps: Step 1, "Choose a VIVOTEK service to connect", which is completed (indicated by a blue checkmark), and Step 2, "Choose a location to synchronize devices", which is the current active step (indicated by a blue circle with the number 2). Under Step 2, there are two dropdown menus: "Organization" with the placeholder text "Select an Organization" and "Site" with the placeholder text "Select a Site". At the bottom of the dialog are two buttons: "Back" and "Apply".

Log off from Server

Click  and select **Log off**.