Shepherd

User Manual

Product Version: v3.6 | Document Version: v3.6

VIVOTEK
A Delta Group Company

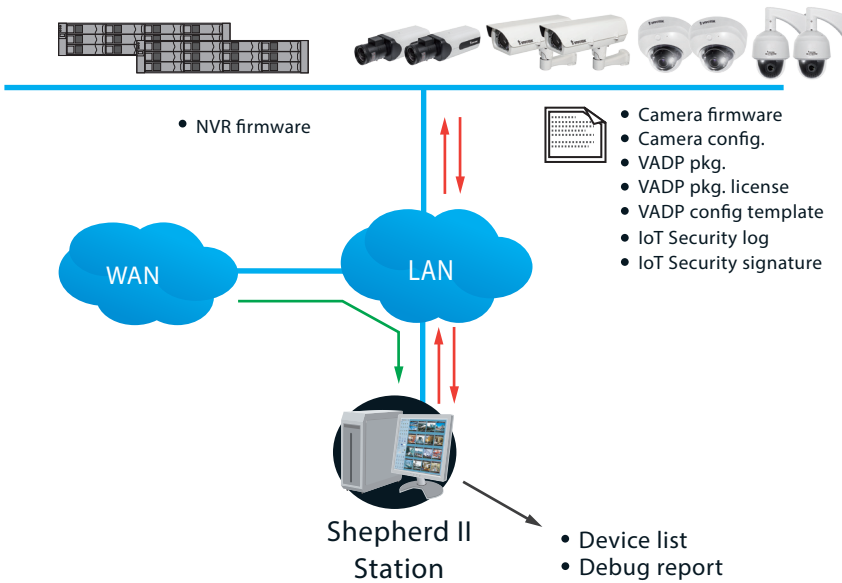
About this Document

Rev. 1.0: This document is written for Shepherd revision 2.1.0.0 or later.
Rev. 1.1: Added the IP range search function.
Rev. 1.2: Added description for the forceful password policy.
Rev. 1.3: Added description for the adaptive resolutions, the Debug report, the support for Smart Stream II, default and selectable browser support, and DRM information. Renamed Shepherd II as Shepherd.
Rev. 3.2: Added Batch NVR firmware upload, NVR device list export, Batch package config setup, Batch Trend Micro IoT package setup, and Exceptions for restoring to factory defaults.
Rev. 3.3: Added the Import and Export LPR package feature, and SD card management.
Rev. 3.4: Supports resize, maximize, and restore the window size.
Added the display of camera Host name.
Supports UI text language update.
Selectable package download to SD card or camera flash memory.
Rev. 3.6: Added new features available with software revision 3.6.0.1 or later.

Table of Contents

How It Works

The Shepherd utility is an installation and management tool that helps facilitate the configuration of multiple cameras. The tool can be used to automatically search the network for cameras, assign IP addresses, display connectivity, manage firmware/software upgrades, and collectively configure multiple cameras.



I. Requirements

Shepherd supports Windows OSes. You should upgrade your operating system with the latest service packs:

- Windows 10, 8, 7

- Below are the typical TCP ports for access to individual network cameras

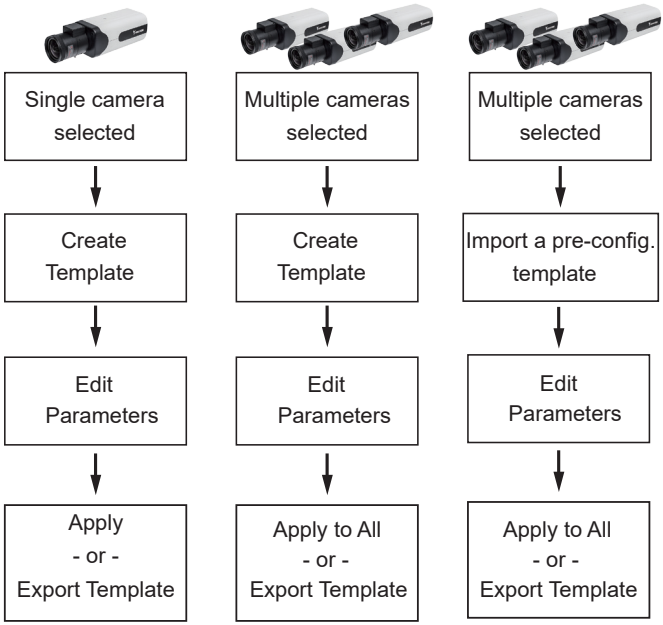
Network General settings:

HTTPS =	443
FTP =	21

Streaming:

HTTP =	80
Secondary HTTP =	8080
RTSP =	554
RTP for video =	5556
RTCP for video =	5557
RTP for audio =	5558

- To start using the Shepherd utility, you can select one or multiple cameras to create a new template, and then edit the detailed parameters. If you already have a standard template, you can import the template and then apply it to one or multiple cameras.

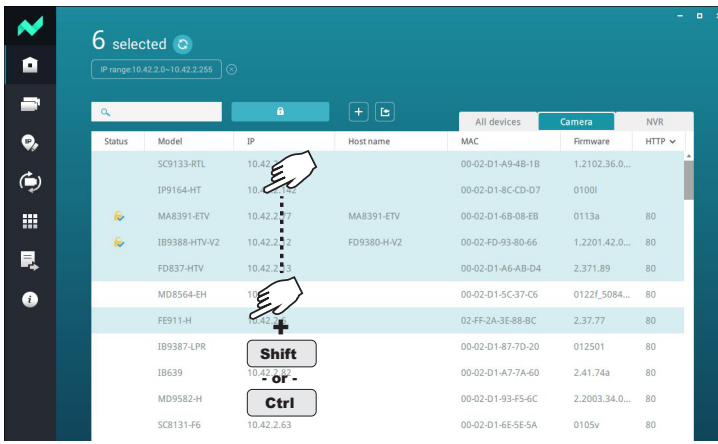


VAST server and NVR will also appear on the device list. However, they can not be selected for configuration.

II. Configuration Procedure

1. A few seconds after the utility is started, all cameras in the same subnet should be listed on the home page. Shepherd can locate cameras residing in the same network section having the same first two address octet values, such as "172.18.x.x."

2. You can then use the combination of mouse clicks and the **Shift** or **Ctrl** keys to select one or multiple devices.



Ctrl + **A** to select all cameras.

You can access the devices outside your current subnet by manually entering their IP address. 

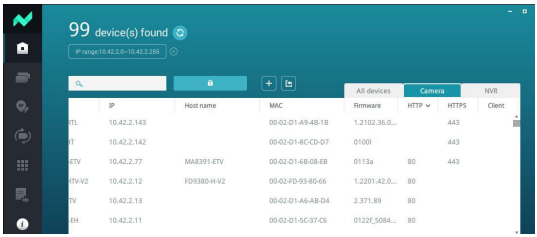
If you have a **Device list** you previously exported to the computer, you can also use the Device list to quickly access the cameras saved into your configuration profile. A Device list created on another Shepherd instance in a different subnet can also be used for access to the cameras in a different subnet.

You can use the **Camera** tab to check the statuses of selected cameras, or use the **NVR** tab to check the statuses of all NVRs.

Each connected camera will be displayed with the following information:

- **Status**: An online icon  is displayed when the device is connected. This icon will be absent if the Shepherd utility cannot connect the device.
- **Model**: The device's model name.
- **IP**: The device's IP address. Note that if devices cannot acquire IP addresses from a DHCP server, the devices will assume the default 169.254.x.x addresses.
- **MAC**: The MAC address that comes with the device.
- **Firmware**: The firmware revision number.

If you need to open a web console to a device, double-click on the device's entry on the list.



Double-click to open a web console to a device. The default browser is IE. Use the **F10** key to open the web console with the system's default browser.

The **HTTP**, **HTTPS**, and **Client** port number will display at the end of row. VIVOTEK NVRs allow access from the VAST CMS software or iViewer. The Client port displays the port number for access. The Client port displays for NVRs running firmware rev. 2.2.0.1 and later.

With many cameras in the subnet, you can use the search panel to locate specific cameras:

1. By entering a part of their model names, such as:
   - "IP" for VIVOTEK's outdoor bullets or box cameras.
   - "FD" for fixed dome,
   - "SD" for speed dome,
   - "IB" for later outdoor bullets, etc.

   Any alpha-numeric characters in the model name can be used as the search condition.

2. The list of devices can also be narrowed down using IP address as the search condition; e.g., entering 172.18.202.x. Only the devices with the same Class C addresses will be listed.

3. MAC address and firmware revision number can also be used, provided that a dash, "-", should be used between every dual digits in the MAC, e.g., "31-b4."

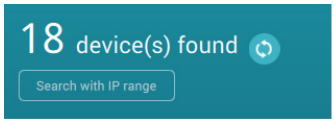
4. You can combine the search conditions using a space. For example, enter "202.x IP83", and then only the cameras belonging to the IP83xx series in the 172.18.202.x subnet will be listed.

You cannot directly manage a VIVOCam PoE switch. However, you can search and then double-click to open a web console to it.

Shepherd automatically detects screen resolution and chooses the appropriate display size. If you want to manually change the display resolution, e.g., using a small window on a 4K monitor, press the **F11** key to change the resolution.

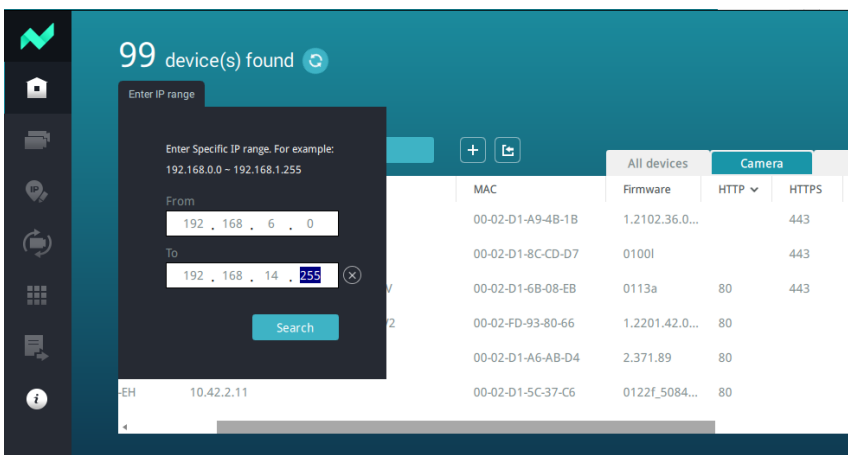
Shepherd window size	Monitor resolution
800 x 600	W1112 x H768
1112 x 768	Normal display condition
2227 x 1533	W3840 x H2000.

IP range search



The Search with IP range function can search within a network section having the same first two address octet values, such as "172.18.x.x." Default is 0.0.0.0. You should manually enter the IP address, and choose to enter an end range. Note the following when using the search function:

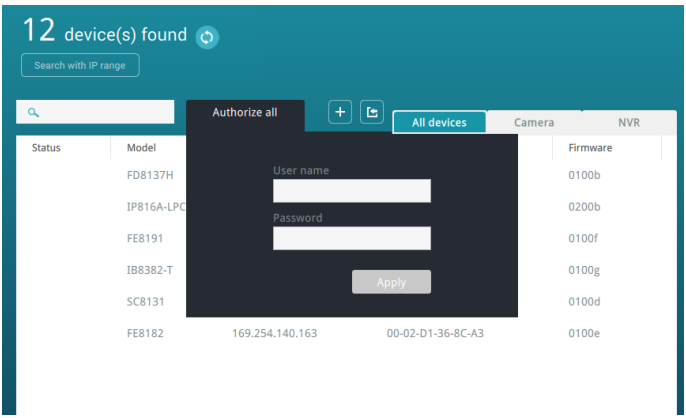
1. When using a single subnet as a search condition, you can enter the asterisk mark, "*", as the search condition; e.g., 192.168.6.*.
2. Use the Tab key to move from one octet value to another.
3. You can search across multiple subnets by specifying a From and a To addresses; e.g., From - 192.168.6.0 and To - 192.168.40.255.
4. If the From and To addresses are used to search across multiple subnets, you cannot use the asterisk * mark.
5. You can specify 172.*.1.1 as the IP range. Then all devices between 172.0.1.1~172.255.1.1; namely, 172.0.1.1, 172.0.1.2 ..... , to 172.254.255.255, 172.255.1.1 will be listed.
6. You can not leave any of the octet fields empty.



Note that a large IP range takes longer for the utility to display the search result. If a range is larger than 100,000 addresses, search will be abandoned.

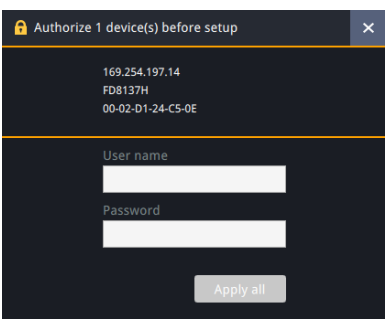
For devices protected by preset passwords, left-click to select it and click the **Authorize** button. This authorizes the access to the device for it to be selected for further configuration. The authorization of cameras can be processed in both All devices and Camera tab, however, the authorization of NVRs can only be performed in the NVR tab.

Without the Authorization, you will be prompted for a password every time you select the device for configuration.



Without the authorization, the credential prompt will appear every time the device is selected for any of the functions.

Note that only the following alpha-numeric characters are supported for passwords:
a-z, A-Z, 0-9, !%-.@^_~

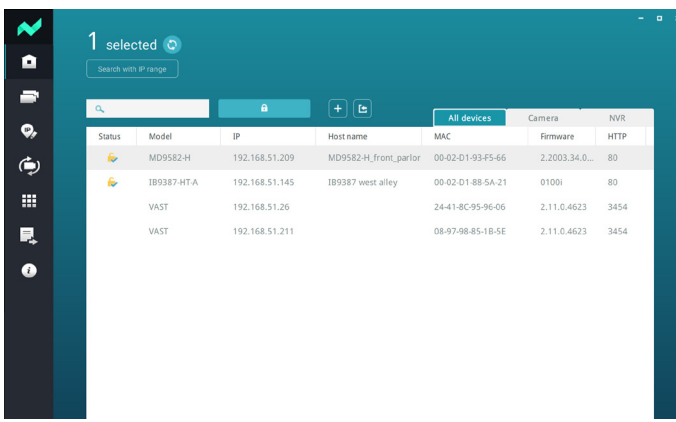


The following characters can not apply in all functional configuration windows:
‘’ “ < > & = ; | ` $ ( )

Once authorized, an online icon appears at the front of the devices. You can authorize multiple devices at one time. However, you can only authorize NVRs in the NVR tab.

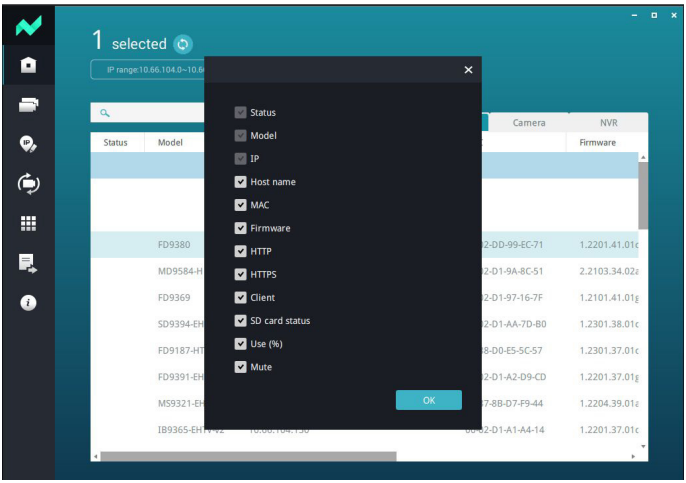
Status	Model	IP	MAC	Firmware
	AW-GET-094A-1...	192.168.4.162	00-02-D1-2F-B7-3C	0106
	FD8166A-S	192.168.4.158	00-02-D1-3D-A8-6A	0200u
	FE9391-EV	192.168.4.116	00-02-D1-5C-1A-84	0100f_22_a
	IB9367-HT	192.168.4.171	00-02-D1-5C-3A-63	0100e
	FD8365-HTV-v2	192.168.4.157	00-02-D1-62-89-BE	0101a_sam...
	IB9365-HT	192.168.4.185	00-02-D1-62-8A-DC	0101b

The authorized cameras will display their host names if those names have been separately configured for the camera, e.g., FE9192 on the front parlor. If a name is too long, the abbreviation mark "..." will be used instead. This feature is available since rev. 3.4.

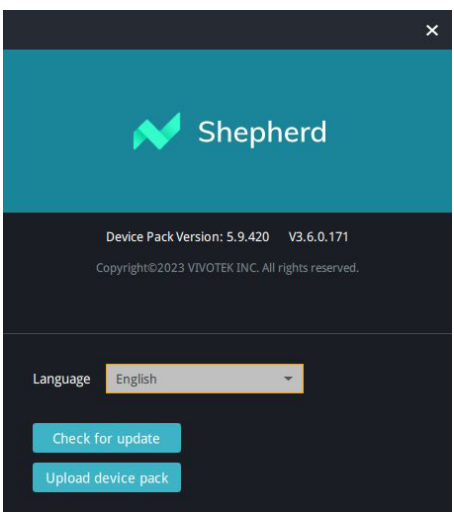


As long as Shepherd is open, the authorized status will remain effective even after switching between different network segments. In other words, you do not have to reenter the user name and password once a device has been authorized.

You can also right-click the title bar to show or hide the columns you want to see.



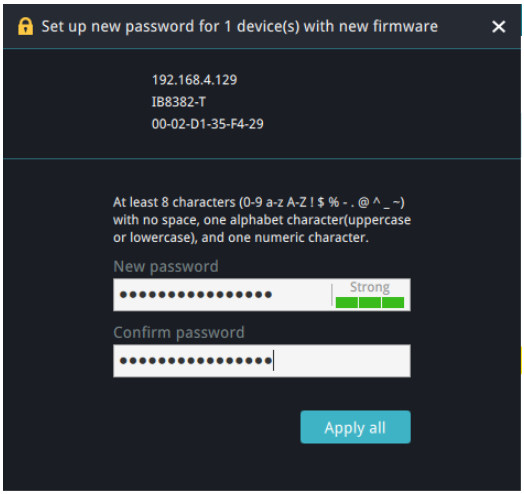
In addition, on the Information page, you can let Shepherd support new device models by uploading a device pack file (*.vdp).



Forceful Password Configuration

When you impose a new password to one or multiple cameras (the Authorize function), Shepherd will prompt for a password configuration for security concerns.

Enter the combination of alphabetic and numeric characters to fulfill the password strength requirement. The default name for the camera administrator is “root.”

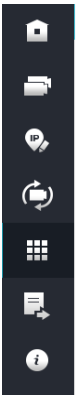


Some, but not all special ASCII characters are supported: !, %, -, ., @, ^, _, and ~.
You can use them in the password combination.

Passwords must be at least 8 characters in length. The combinations of alphabetic and numeric characters determine the strength of your passwords. The more complicated or more random the combination, the higher the strength. At least 1 upper case, numeric, and special character must be embedded somewhere in the middle of the password.

IMPORTANT:

All functional windows under the Home page will only become usable when at least one camera is selected.

	Camera Functional Windows
	Home (Main)
	Batch camera setup
	Assign IP automatically
	Maintenance
	VADP (VIVOTEK Application Development Platform)
	Export device list & debug report
	Information

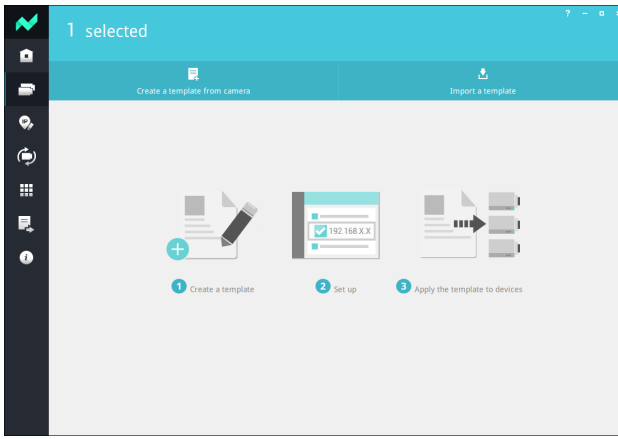
	NVR Functional Windows
	Home (Main)
	Maintenance
	Export device list & debug report
	Information

NOTE:

- Cameras of different models and firmware can be selected for the configuration.
- When parameters have been changed, such as those for Audio or Stream settings, all applicable changes will be applied to all selected cameras. For changes that cannot be applied to specific cameras, e.g., changing a video stream to MPEG-4 on a model that does not support MPEG-4, the changes will be automatically ignored.

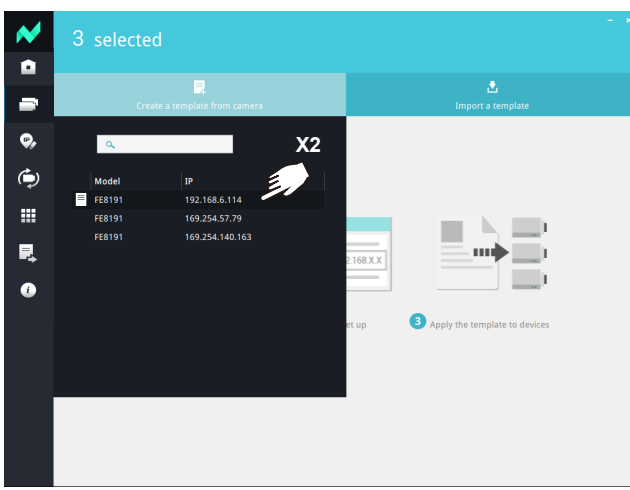
1. With selected cameras, you can start configuring camera parameters, IP addresses, upgrade firmware, reset, restore, etc. Click on the functional icons on the left of the screen.

   - Click on **Batch camera setup** on the left panel.
   - Click on **Create a template from camera**; or, if you already have a template, click on **Import a template**.

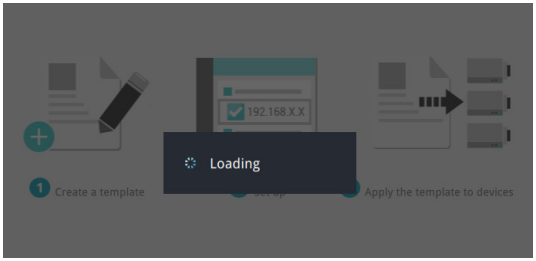


2. Select one camera from the drop down list. Double-click to select a camera. Configuration will begin using the camera's configuration profile. The parameters should only be modified by experienced users.

Note that not all camera parameters can be accessed from Shepherd.

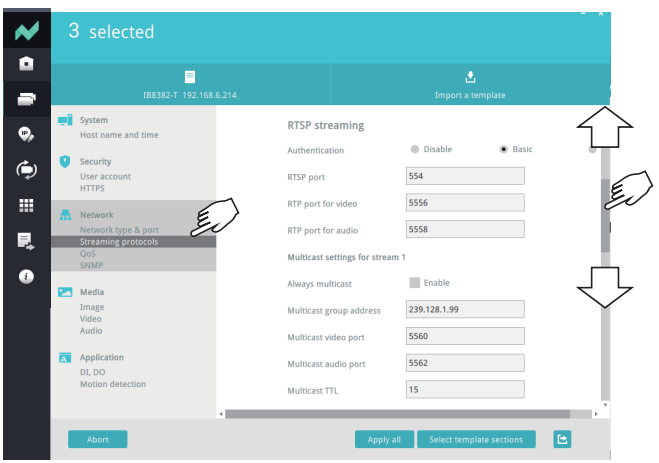


It takes a short while to access and retrieve the camera's configuration.



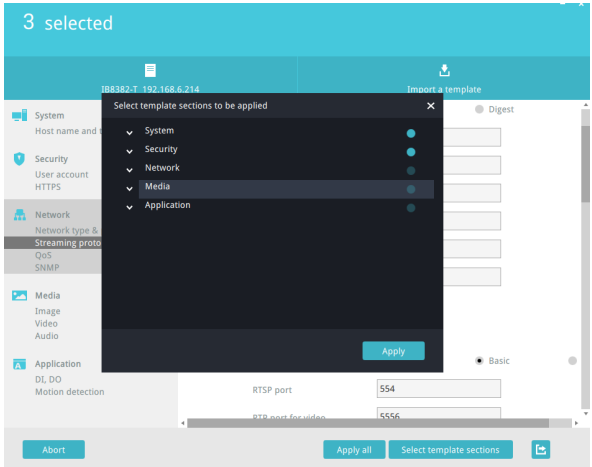
3. The configuration page will appear with sub-windows starting from System, Security, Network, Media, and Application.

- For details about each configurable option, please refer to the documentation that came with each camera.
- The sub-windows contain numerous options. Use the scroll bar on the side to access all of the options.



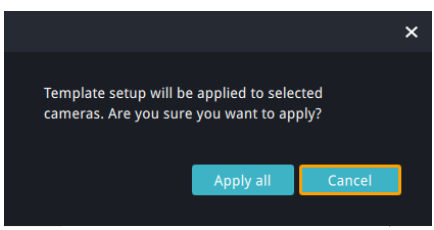
Note that for cameras that support Smart Stream II, the Smart Codec configuration only supports the Auto Tracking mode. The Manual mode and Hybrid mode are not configurable on Shepherd.

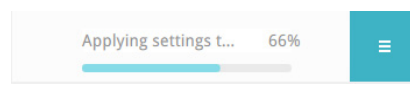
You may not need to apply all parameter changes to cameras. When applying changes in parameters, you can use the **template section** selector at the bottom of the screen to designate the sections to apply.



4. When you finish editing the configurable parameters, click the **Apply all** button to apply changes to selected cameras, or click the **Export** button to save changes to a template. The camera configuration template will be saved in a csv (Comma Separated Values) file.

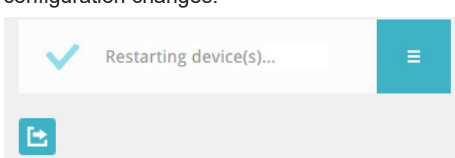
To abandon the changes, click the **Abort** button.





If problems occur when applying the changes, e.g., due to a connection problem, you can use the restart button to retry the apply process.

You may then return to the Home page, or click the **Export** button to save your configuration changes.

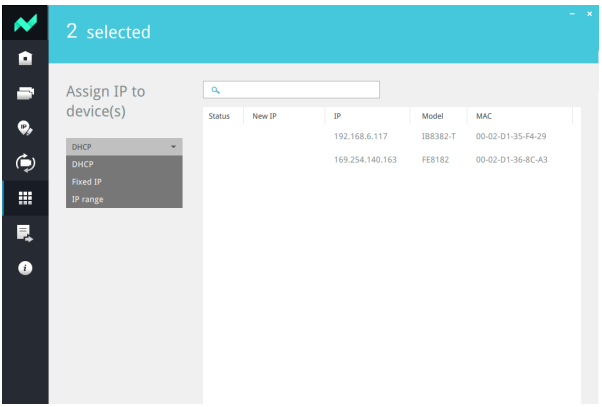


Assign IP

In here, you can assign IP addresses to one or multiple devices.

- IPs can be obtained automatically from a DHCP server.
- IPs can be assigned with an IP address range.

Note that when manually assigning a fixed IP, you should select only one camera.



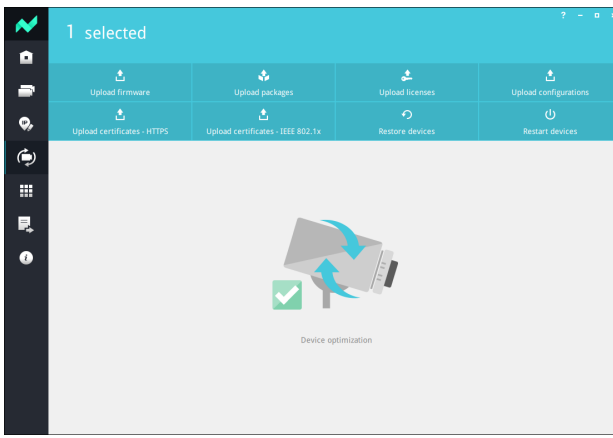
Consult your network administrator for network settings. Also ensure the correct Gateway and DNS server addresses are provided.

Maintenance

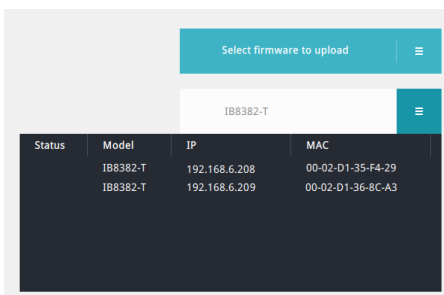
One or more cameras can have its firmware, license, and packages (VCA packages, such as line/field detection, or people counting) updated via this page. Cameras can also be reset or restored to its defaults.

Select the cameras to be configured from the home page, click on the **Maintenance** button, and then click to perform one of the update functions from the top menu.

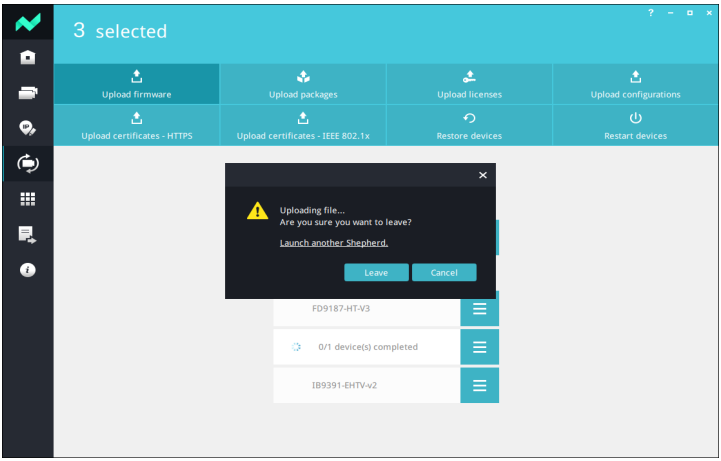
Please note that the firmware, software license, and software packages should be manually downloaded to the client computer running this utility. The Shepherd utility does not automatically search for the latest updates.



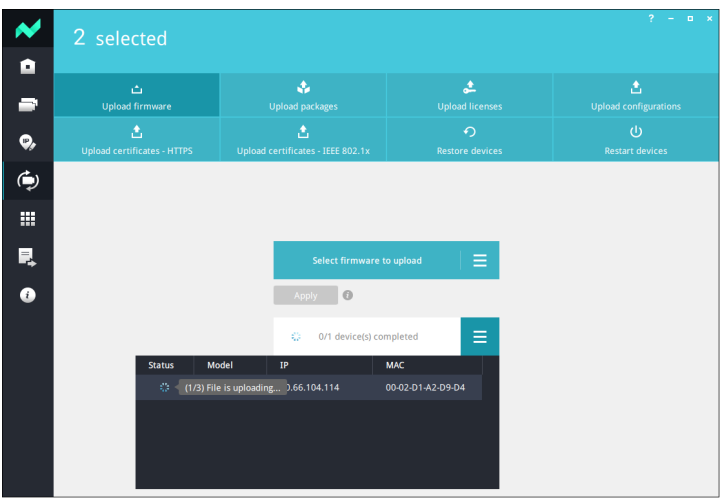
Upload firmware
Select a firmware/software file for the listed model on screen. If you have multiple cameras of the same model, they will be listed using the List button on the right. You can then upload their firmware at the same time.



While uploading a firmware file, you can open another or more Shepherd instances to work on other cameras simultaneously. To do so, click Open one more Shepherd for other tasks in the dialog box below.



While firmware is updating, you can see the status and tooltip (as shown below) for you to realize the firmware updating progress.



The following three tooltips show each normal status of the firmware updating progress:

1. **File is uploading**: Shepherd is uploading the firmware file to the camera. Note that this process may take longer in a limited network environment. You can adjust the parameters of pipelinedUploaders and uploadFirmwareTimeoutMs in the settings.ini explained in Appendix if needed.

2. **Camera is updating:** The camera is unzipping and updating the firmware itself. (Note that this process may take longer for C-series camera models.)

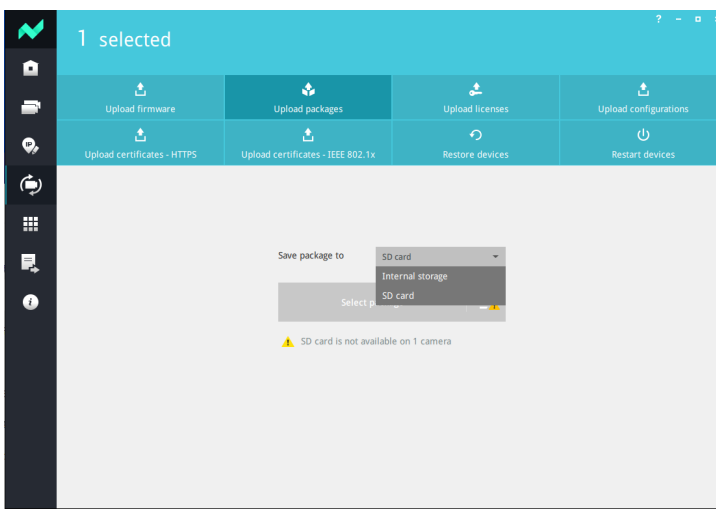
3. **Camera is reconnecting:** The camera finishes updating configuration and starts rebooting. (Note that this process may take longer for C-series camera models.) You can adjust the parameter of verifyRestartTimeoutMs in the settings.ini explained in Appendix if needed.

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

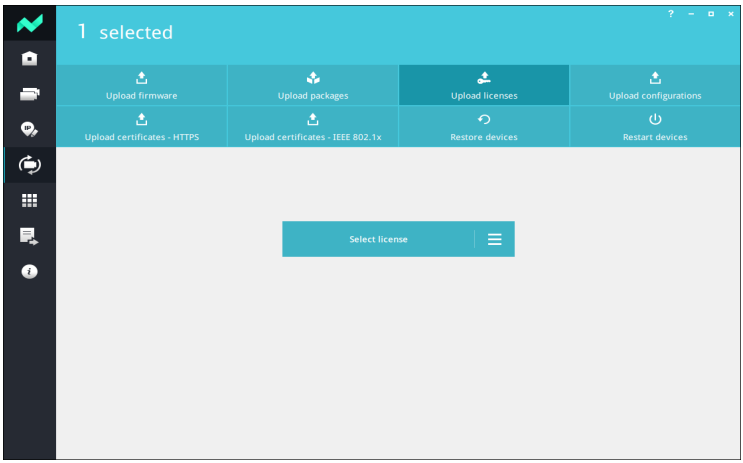
1. **Invalid file for this model group:** The firmware may not correspond to the camera model or is incompatible.
2. **File upload timeout:** The upload process took longer than the expected/ specified time. You can adjust the parameters of pipelinedUploaders and uploadFirmwareTimeoutMs in the settings.ini explained in Appendix if needed.
3. **Failed to connect to device:** The upload process was interrupted because of unstable network environment.
4. **Device response timeout or IP changed after rebooting:** Possible causes may be that the update time exceeded the timeout, the camera IP address change could not detect if update is successful or resulted in no detection of the camera, or other abnormality occurred.

Upload packages

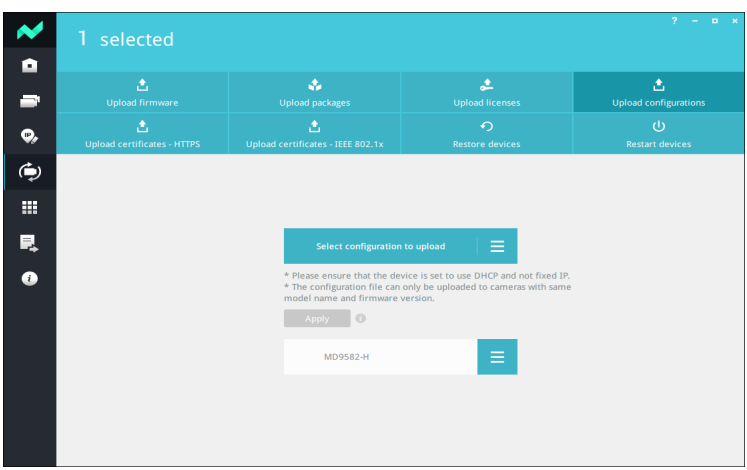
When uploading a package, you can select to upload to a camera's flash memory or an SD card that has already been installed.



Upload licenses
You can upload the license file (*.txt or *.json) of a particular device to apply to all other devices of the same model.



Upload configurations
You can upload the configuration file of a particular camera to apply to all other cameras of the same model.



The following two tooltips show each normal status of the configuration updating progress:

1. **File is uploading:** Shepherd is uploading the configuration file to the camera. Note that this process may take longer in a limited network environment. You can adjust the parameters of pipelinedUploaders and uploadFirmwareTimeoutMs in the settings.ini explained in Appendix if needed.

2. **Camera is reconnecting:** The camera finishes updating configuration and starts rebooting. (Note that this process may take longer for C-series camera models.) You can adjust the parameter of verifyRestartTimeoutMs in the settings.ini explained in Appendix if needed.

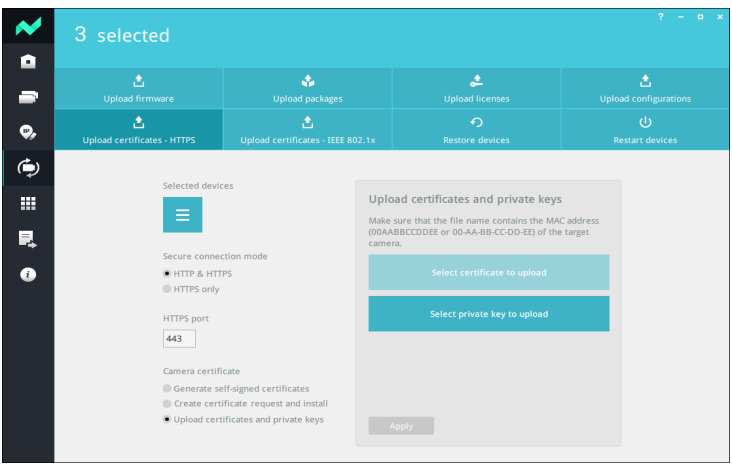
If configuration update fails, one of the following tooltips may appear. Please find a suitable solution to solve the indicated problem.

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/specified time. You can adjust the parameters of pipelinedUploaders and uploadFirmwareTimeoutMs in the settings.ini explained in Appendix if needed.
3. **Failed to connect to device:** The upload process was interrupted because of unstable network environment.
4. **Device response timeout or IP changed after rebooting:** Possible causes may be that the update time exceeded the timeout, the camera IP address change could not detect if update is successful or resulted in no detection of the camera, or other abnormality occurred.

Upload certificates - HTTPS

For all selected authorized cameras, you can upload their HTTPS SSL certificates all at once:

1. Select authorized cameras.
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:
   - **Generate self-signed certificates:** Select this if you want to use self-signed certificates created, issued, and signed by VIVOTEK.
   - **Upload certificates 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 files. Select this if you have certificate files ready. Note that the file name should contain the MAC address (00AABBCCDDEE or 00-AA-BB-CC-DD-EE) of the target camera.
   - **Upload certificates and private key:** Select this if you have both certificate and private key files ready.



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 user-selected files is fewer than the number of cameras to be updated, or that some file names do not contain the MAC address.

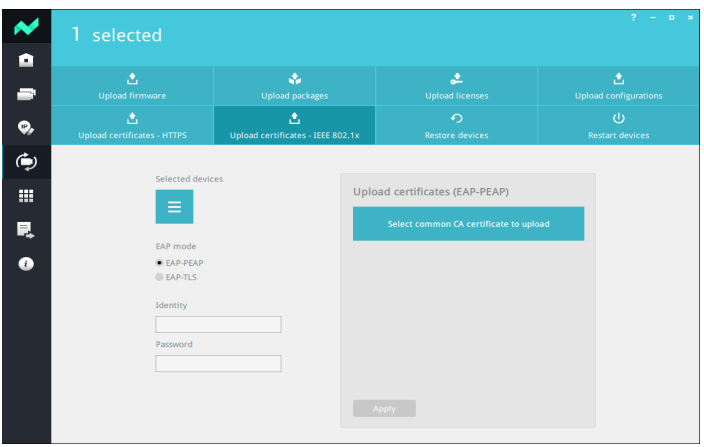
Upload certificates - IEEE 802.1x

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

1. Select authorized cameras.
2. Select **EAP-PEAP** or **EAP-TLS** as the EAP mode and its corresponding certificate files.
   - **EAP-PEAP:** based on server-side certificate authentication
   - **EAP-TLS:** based on client certificate authentication
3. Click **Apply**.

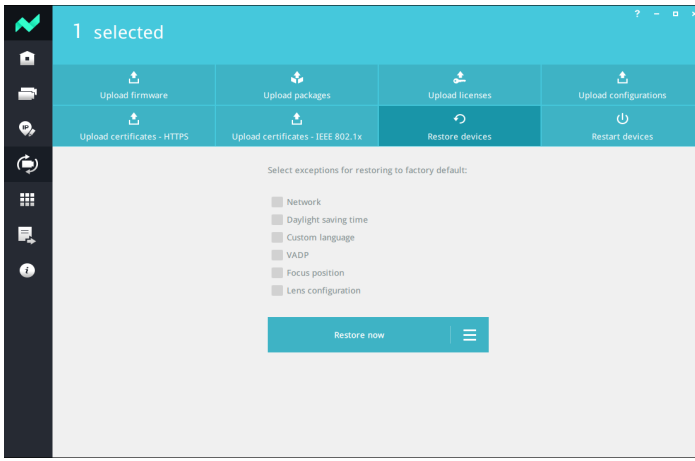
If IEEE 802.1 certificate upload fails, one of the following messages may appear. Please find a suitable solution to solve the indicated problem.

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 user-selected files is fewer than the number of cameras to be updated, or that some file names do not contain the MAC address.

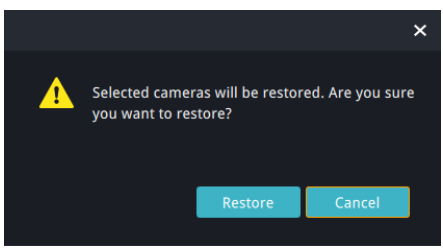


Restore devices

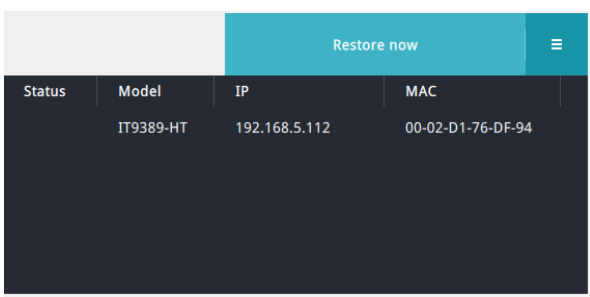
If you need to restore a camera's firmware defaults, you can select to preserve some of the current parameters without restoring all to defaults. They include: Network parameters, Daylight saving time, Custom language, VADP, Focus position, Lens configuration.



A confirm box will appear. Click **Restore** to proceed.



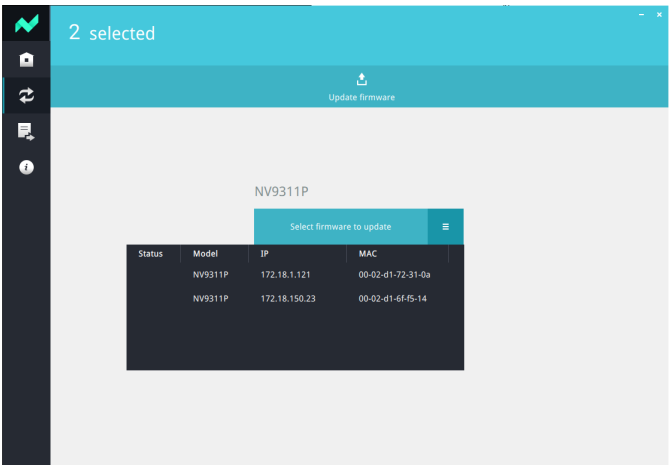
You can use the **List** button by the side of the Restore button to check out the device whose defaults will be restored.



Maintenance - NVR Related

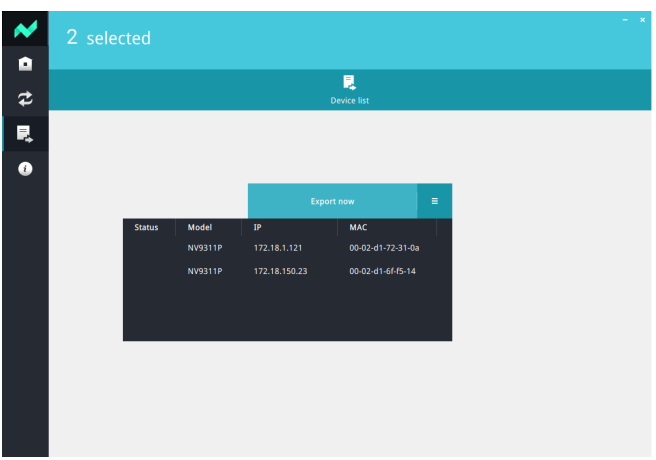
Firmware Update - You can select one or multiple NVRs, click Maintenance, and update their firmware at once.

Select the NVRs to be configured from the home page, click on the **Maintenance** button, and then click to perform one of the update functions from the top menu.

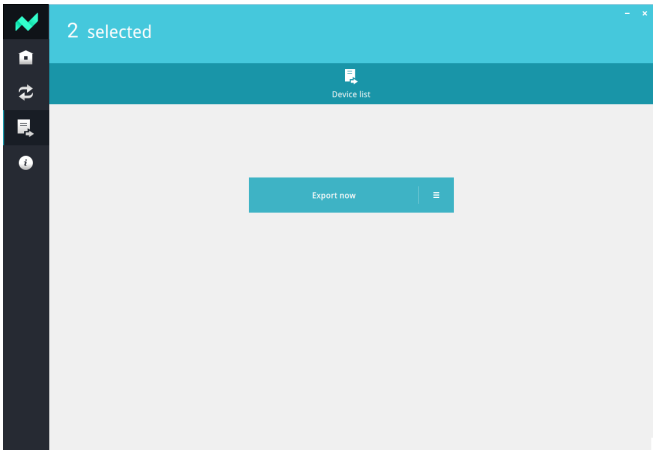


Export Device List -

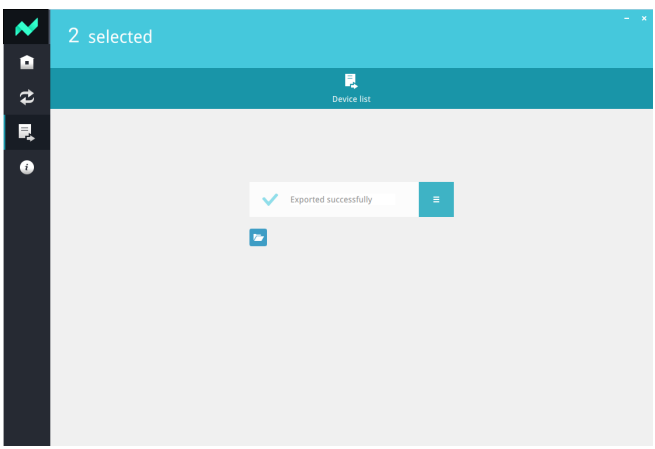
1. Select an NVR.
2. Click **Export device list and debug report**.



3. Click **Device list**, and click **Export now**.



4. The Exported successfully message will prompt. You can click the location button to access the device list.

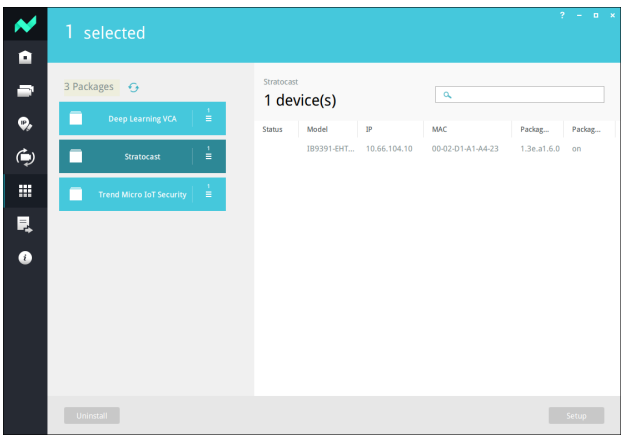


VADP

VADP may include VIVOTEK's or 3rd-party applications, such as Deep learning analytics and Trend Micro IoT security packages.

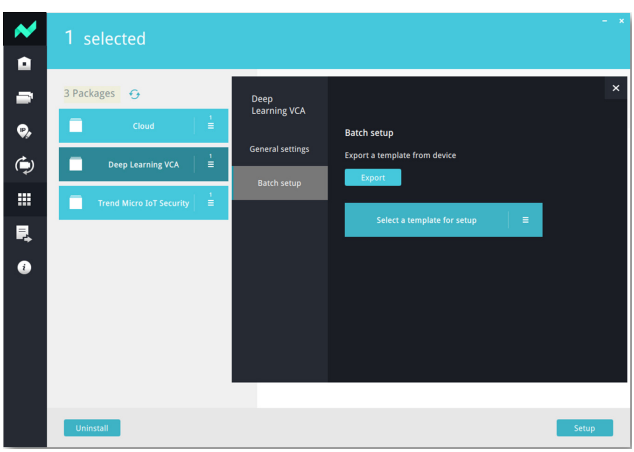
You can enable/disable an individual VADP module, uninstall, or export a configuration template. Some configurations, e.g., a people counting configuration for a train door, can be exported and applied to the identical doors of a train.

Please note that the software packages should be manually downloaded to the client computer running this utility. The Shepherd utility does not automatically search for the latest updates.

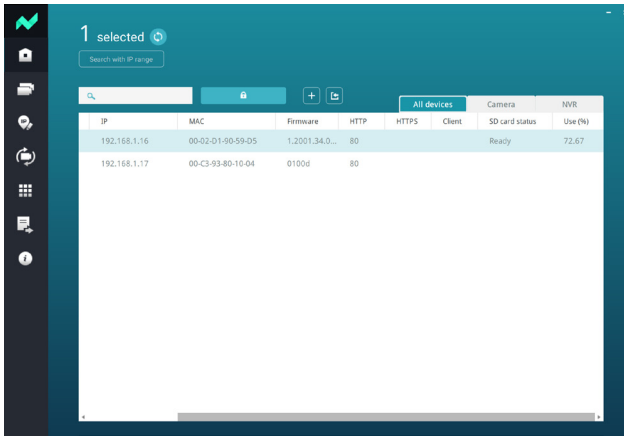


Please note that currently Shepherd does not support the VADP package setup for the Cloud package.

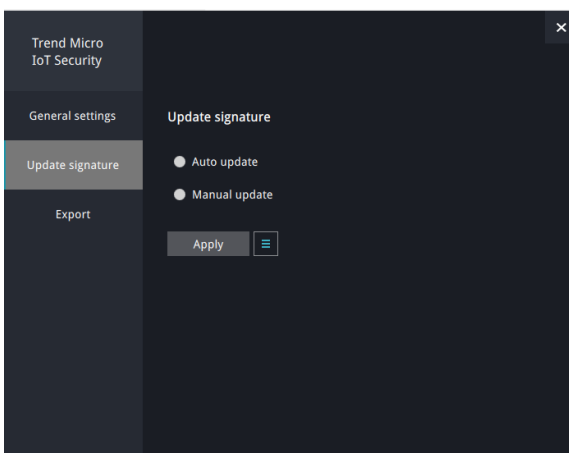
You can select to configure the VADP modules onboard one or multiple cameras. You can enable, disable, or uninstall the VADP packages. The batch setup feature only applies to Stereo Tracker, Deep Learning VCA and VCA package.



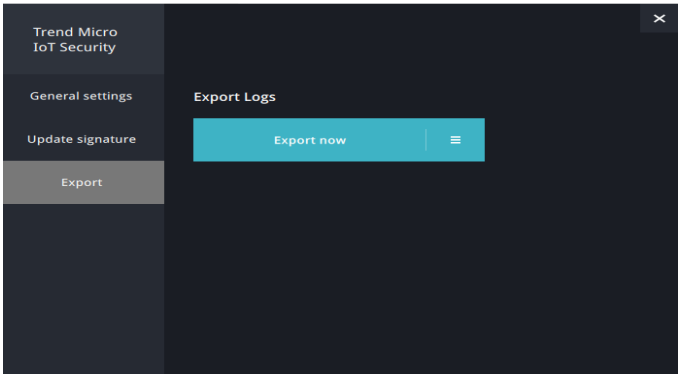
If the camera comes with an SD card, the package will be uploaded to the SD card. You can see its status at the camera information columns.



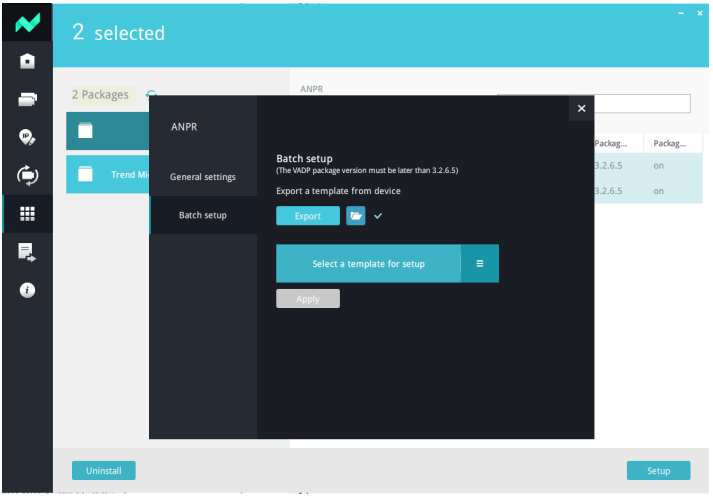
You can select **Trend Micro IoT Security** and update the signature (virus and malware database updates). You can manually update the signature or let cameras automatically update to the latest signatures.



The **Export log** function in this window allows you to export system events that are related to cyber attacks or others that are related to security breaches.



For VIVOTEK's LPR cameras, this page can also be used to upload the LPR software package. Download a new package and batch upload the new package to your LPR cameras.

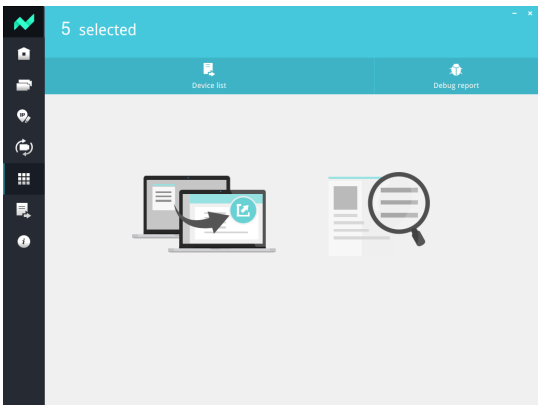


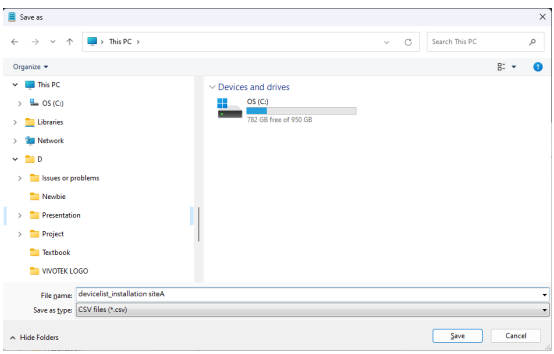
Export Device List and Debug Report

This window contains the following:

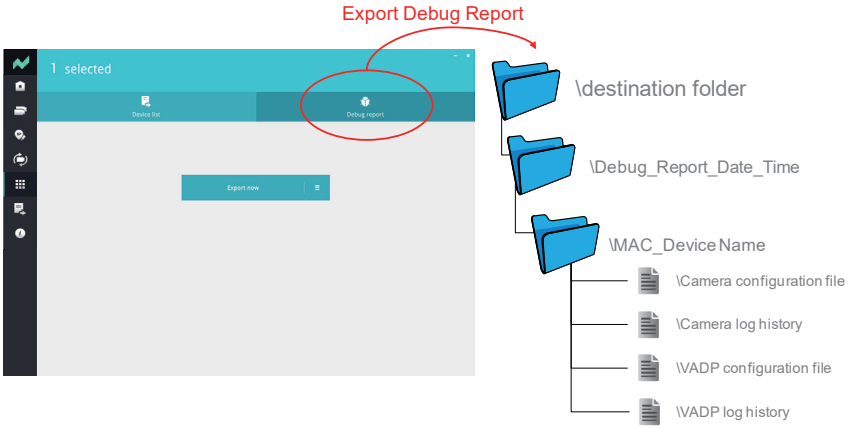
- A **Device list** contains information of selected cameras. You can also import a previously-saved device list from the home page to connect and select all cameras from an established deployment. This is especially the case if your deployment include cameras residing in different subnets.
- A **Debug report** contains event messages, log history, connection statuses, and configuration file that facilitate problem solving if the need should arise when you need to contact VIVOTEK's technical support. VCA (Video Content Analysis) Package information is also included.

Note that when you export a debug report, you need to create a new file folder to contain the debug report.





The debug report contains the following:

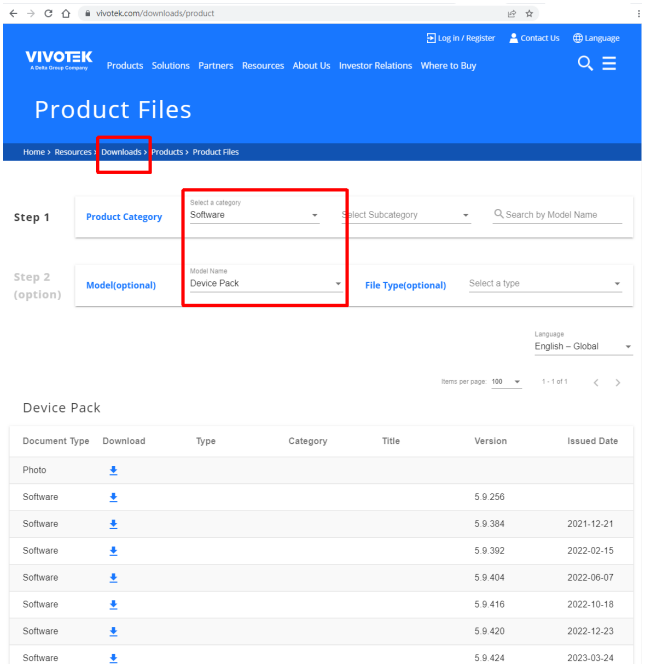


Information

The information page provides access to the UI text Language selector and an automatic update search button for the utility. You can also upload an updated device pack as needed.

Device Pack

To update a device pack that contains information for the latest VIVOTEK cameras,
1. Download the latest device pack (*.vdp) from VIVOTEK website.



2. Save the file and decompress it to the same folder where the Shepherd.exe file is located. Restart the Shepherd utility. The Shepherd utility will automatically accommodate the latest parameters brought by the device pack file.

Appendix: Adjust settings.ini

Shepherd provides advanced parameters that can be adjusted to suit different network environments. Follow the steps below to adjust these parameters as needed:

1. Locate the settings.ini file in the Shepherd folder.
2. Open the settings.ini file and find the following parameters:
   - **pipelinedUploaders (number):** Adjust this parameter to upload firmware to all selected devices (0) or to a specified quantity of devices at a time (N). For example, pipelinedUploaders=16 means Shepherd will upload firmware to the first 16 devices and then upload to the next 16 devices until the upload process of the first 16 devices is finished.
   - **uploadFirmwareTimeoutMs (millisecond):** The default value is 600,000 milliseconds (=600 seconds=10 mins), which means Shepherd will determine it is a failure when the firmware uploading process takes more than 600 seconds. You can adjust this value based on a device's capability or the network speed limitation.
   - **verifyFirmwareTimeoutMs (millisecond):** The default value is 30,000 milliseconds (=30 seconds), which means Shepherd will determine it is a failure after checking the firmware version with a device and the device has no response within 30 seconds.
   - **verifyFirmwareSleepMs (millisecond):** The default value is 20,000 milliseconds (=20 seconds), which means Shepherd will check the firmware version with a device every 20 seconds.
   - **verifyRestartRetryTimes (number):** The default value is 20 times, which means Shepherd will determine it is a failure after checking the firmware version with a device (which is rebooting after updating the firmware) 20 times and the device has no response.
   - **verifyRestartTimeoutMs (millisecond):** The default value is 30,000 milliseconds (=30 seconds), which means Shepherd will determine it is a failure after checking the firmware version with a device (which is rebooting after updating the firmware) and the device has no response within 30 seconds.
   - **verifyRestartSleepMs (millisecond):** The default value is 20,000 milliseconds (=20 seconds), which means Shepherd will check the firmware version with a device (which is rebooting after updating the firmware) every 20 seconds.
3. Adjust the parameters as needed.