DVTEL INC.
65 Challenger Road
Ridgefield Park, NJ 07660

DNA 2.0
User Manual

dvtel® Now you can.

Rev H3 October 30, 2014

Table of Contents

Revision History

Version	Date	Author	Comments
A	Jun. 26, 2012	Alan Singer	For software version 1.0.3.1 (beta). First release.
B	Aug. 15, 2013	Alan Singer	For software version 2.0.0.9. Added support for Quasar 2MP cameras; Quasar CM-4321 camera; Ariel EN-204 encoder; Quasar PTZ head firmware upgrade; storage space requirement; Windows 8 and Windows Server 2012; Change Video Format option.
C	Nov. 21, 2013	Barry Klatzkin	For software version 2.0.2.4. Added support for CF-4251 and CM-4251. Added note regarding WinPcap component required to support EN-204 encoder. Updated look and feel.
D-F	November 2013	Barry Klatzkin	General editing (internal versions)
G	Dec. 23, 2013	Alan Singer	For software version 2.0.2.9. Added support for ioimage cameras and encoders. General editing.
H	Apr. 2014	Alan Singer	Added Revision History. Added support for ioimage Thermal CT-5320F, CT-5640F, CT-5320PT, and CT-5640PT cameras; Ariel EN-216 encoder and Ariel CM-3011-01-I camera. Removed Vendor Name column from Discover List, updated Main Screen and Add Device Manually images.
H2	July 13, 2014	Alan Singer	For software version 2.0.4.x. Added support for Ariel CB-3011-01-I camera. Updated sections 4.1.2.1 and 4.1.2.6 to include notes about authenticated Ariel devices. Updated section 4.2.1.4 (Firmware Tab) to include support for ioimage HD cameras.

1 Introduction

This document is intended for administrators and users of DVTEL's DNA (DVTEL Network Assistant) application, which easily discovers and configures edge devices on DVTEL video surveillance systems. The DNA tool has a simple user interface and requires installation only when attempting to assign IP addresses to Ariel edge devices. In this case, you may be required to install WinPcap. This software is provided as a single, standalone executable that runs on any PC.

Supported devices include:

- Quasar cameras
  - CM-3211
  - CM-4221
  - CM-4251
  - CM-4321
  - CP-3211
  - CP-4221
  - CF-3211
  - CF-4221
  - CF-4251
  - CM-6208-11-I
  - CB-6208-11-I
  - CM-6204-11-I
  - CB-6204-11-I

- HD Classic cameras
- HD Elite cameras
- Pro Line MPEG-4 encoders and decoders
- Pro Line A encoders and cameras
- EV series H.264 encoders and decoders
- EA-201 series encoders
- ioimage encoders
- ioimage sc1dn-S and mmp100dn cameras
- Ioimage HD cameras:
  - CF-5222-00
  - CF-5212-00

- ioimage Thermal cameras
  - CT-5320F
  - CT-5640F
  - CT-5320PT
  - CT-5640PT
- Ariel cameras and encoders
  - EN-204 and EN-216 encoders
  - CM-3011-01-I and CB-3011-01-I -cameras

Supported operating systems include 32-bit and 64-bit versions of:

- Windows XP
- Windows 7
- Windows 8 and 8.1 (64-bit only)
- Windows Server 2003
- Windows Server 2008

Windows Server 2012 (64-bit only)

2 Related Documentation

The following documentation contains related information:

- *Quasar Camera Quick Installation Guides*
- *Quasar Camera User and Installation Guides*
- *HD Classic Camera User and Installation Guides*
- *HD Classic Camera Quick Install Guides*
- *HD Elite Camera User and Installation Guides*
- *HD Elite Camera Quick Install Guides*
- *Pro Line MPEG-4 User Installation Guides*
- *Pro Line A User Installation Guides*
- *EV Series Single-Port Encoder Quick Installation Guide*
- *EV Series Single-Port Encoder User Manual*
- *EV Series Single-Port Decoders Quick Installation Guide*
- *EV Series Single-Port Decoders User Manual Guide*
- *EV Series Multi-port Encoders Quick Installation Guide*
- *EV Series Multi-port Encoders User Manual*
- *EA-201 Series Encoder Quick Install Guide*
- *EA-201 Series Encoder User Installation Guide*
- *ioimage encoder and camera Quick Install Guides*
- *ioimage encoder and camera Installation Manuals*
- *ioimage HTML Edition Units User's Guide*
- *ioimage HTML Edition API Reference Manual*
- *ioimage HD Quick Install Guides*
- *ioimage HD User and Installation Guides*
- *ioimage Thermal Quick Installation Guides*
- *ioimage Thermal User and Installation Guides*
- *Ariel EN-204 Quick Install Guide*
- *Ariel EN-204 User and Installation Guide*
- *Ariel EN-216 Quick Install Guide*
- *Ariel EN-216 User and Installation Guide*
- *Ariel CB-3011 Quick Install Guide*
- *Ariel CB-3011 User and Installation Guide*
- *Ariel CM-3011 Quick Install Guide*
- *Ariel CM-3011 User and Installation Guide*

- *Latitude Quick Start Guide*
- *Latitude Quick Reference Guide*
- *Latitude System Components*
- *Latitude System Specifications*
- *Latitude Release Notes*

3 Quick Start Guide

To start using the DNA application

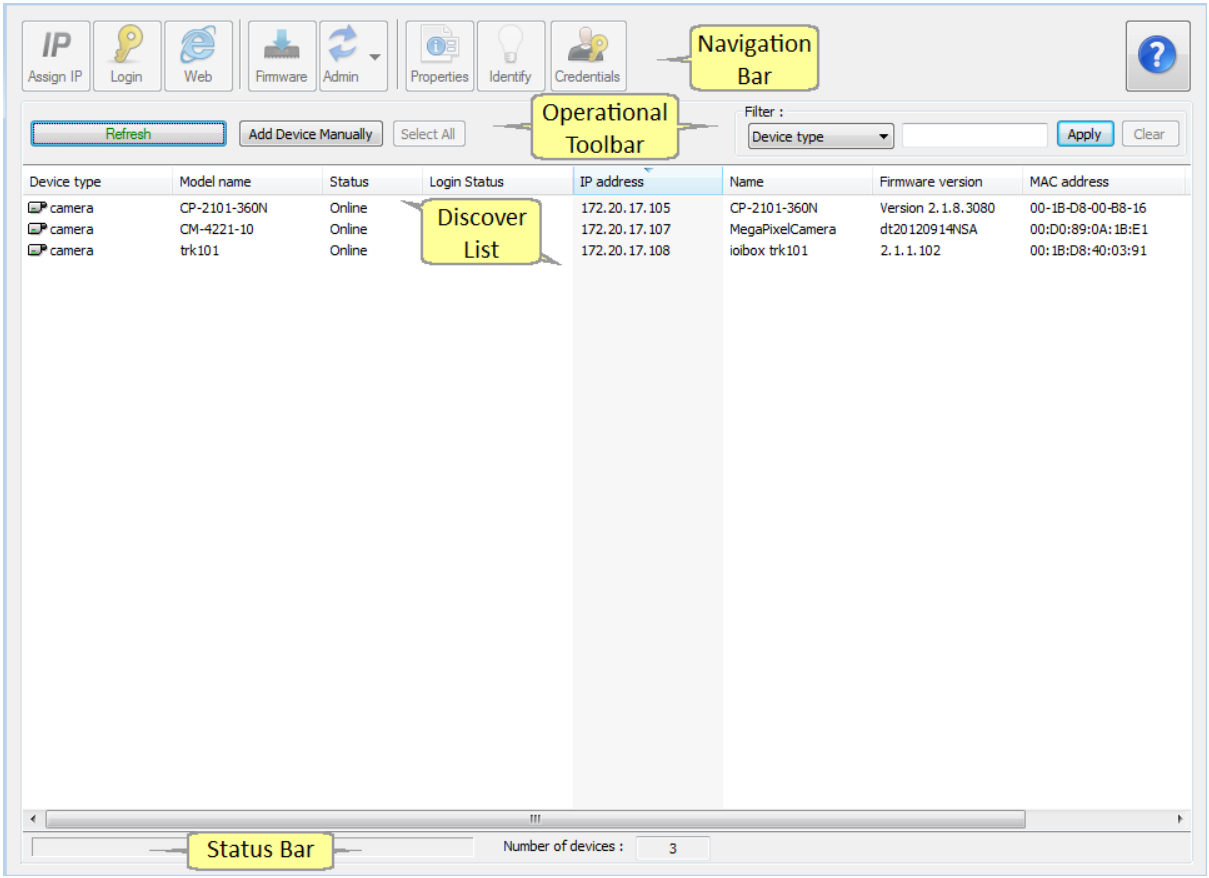
Note:

1. DNA should be run by an account that has User Account Administrator permissions or by an account whose settings have been set to *Never Notify*. Go to Control Panel/Change User Account Settings, and set to *Never Notify*.
2. Ariel devices require installation of an additional component. You are prompted by DNA to run this installation from an account that has administrator permissions.
3. DNA requires 250MB of storage space for a system with up to 1,000 cameras.

1. Run the DNA application on a computer connected to the network. The software is an .exe file.
2. Upon launching the tool, DNA automatically discovers all devices on the same subnet/virtual LAN (VLAN) in the network.
3. In the event that there are devices that are not authenticated, select **Login** and enter login credentials for the devices.
4. If there are devices located on a separate VLAN, the devices must be added manually. Click **Add Device Manually** from the Operational Toolbar and add the devices.

4 Main Screen

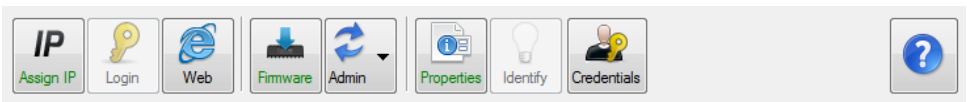
The DNA main screen contains four sections, as seen in the following illustration:



1. Navigation Bar: Located at the top of the screen. Includes tabs and drop-down menus to perform actions.
2. Operational Toolbar: Located below the Navigation Bar. Used to refresh discovered units, filter connected devices for easy operation, and to add a device manually.
3. Discover List: Occupies the center of the screen. Displays a list of discovered devices with partial device information.
4. Status Bar: Located at the bottom of the screen. Displays current device status, including scanning time, status, and the number of discovered units.

4.1 Navigation Bar

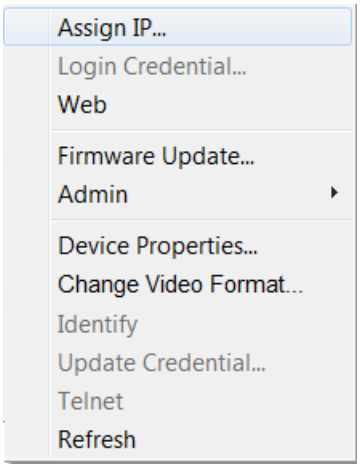
The Navigation Bar contains tabs for all the actions needed to configure and manage attached devices. If no devices have been discovered, all the tabs are gray (disabled). After a device has been discovered, the tabs for functions which it supports are enabled and colored, as seen in the following illustration:



To define the device on which to perform an action, you must select the device from the Discover List. You can select more than one device, in which case the action will be done on all selected devices.

4.1.1 The Context Menu

All functions on the Navigation Bar also are accessible from the context menu, which is available when right-clicking on a device within the Discover List, as seen in the following illustration:



The context menu includes three functions that are not available on the Navigation Bar: **Change Video Format**, **Telnet** and **Refresh**.

1. **Change Video Format:**

The *Change Video Format* option enables the changing of the video format between NTSC and PAL for multiple units. For more information, see Properties Tab (page 20).

> **Note:**
> The *Change Video Format* option is disabled if one or more of the selected devices does not support changing the PAL or NTSC setting.

2. **Telnet**:

The *Telnet* option opens the Telnet application, which accesses the device according to its IP address. The *Telnet* context menu option is enabled (not grayed) when a device is selected from the Discover List, the device is online, and the device type supports this command. You must manually close the Telnet application when finished using the device's Telnet interface.

> **Note:**
> Not all device types support this command.

3. **Refresh**:

The *Refresh* option from the context menu starts the discovery mechanism for devices that are selected from the Discover List. The application displays the last credentials that were authenticated before the refresh operation. A refresh operation can be performed on an individual unit or a group of devices that are selected from the Discover List.

4.1.2 Navigation Tabs

The Navigation Bar includes the following tabs:

- Assign IP
- Login
- Web
- Firmware
- Admin
- Properties
- Identify
- Credentials

In addition, there is a **Help** button on the Navigation Bar.

4.1.2.1 Assign IP Tab

The **Assign IP** tab 

or context menu option is used to assign the IP address of the selected device(s). This function can be used for single-unit or batch network configuration. The **Assign IP** tab or context menu option is grayed if a device has not been selected.

Selecting this tab or option opens the **Assign IP** window, which displays a list of devices which need to be updated, as shown below.

The **Assign IP** window is divided into two areas and includes the following fields:

1. Network details areas:
   - Use DCHP checkbox
   - First IP Address
   - Mask
   - Gateway

Note:

First IP Address, Mask, and Gateway details are gray if the *Use DHCP* checkbox is selected.

2. Status area:
   - Name (device name or model)
   - Current IP
   - Previous IP

Note:

If an Ariel camera or encoder is not authenticated, you must first authenticate it before performing the following steps.

To set DHCP mode on multiple devices

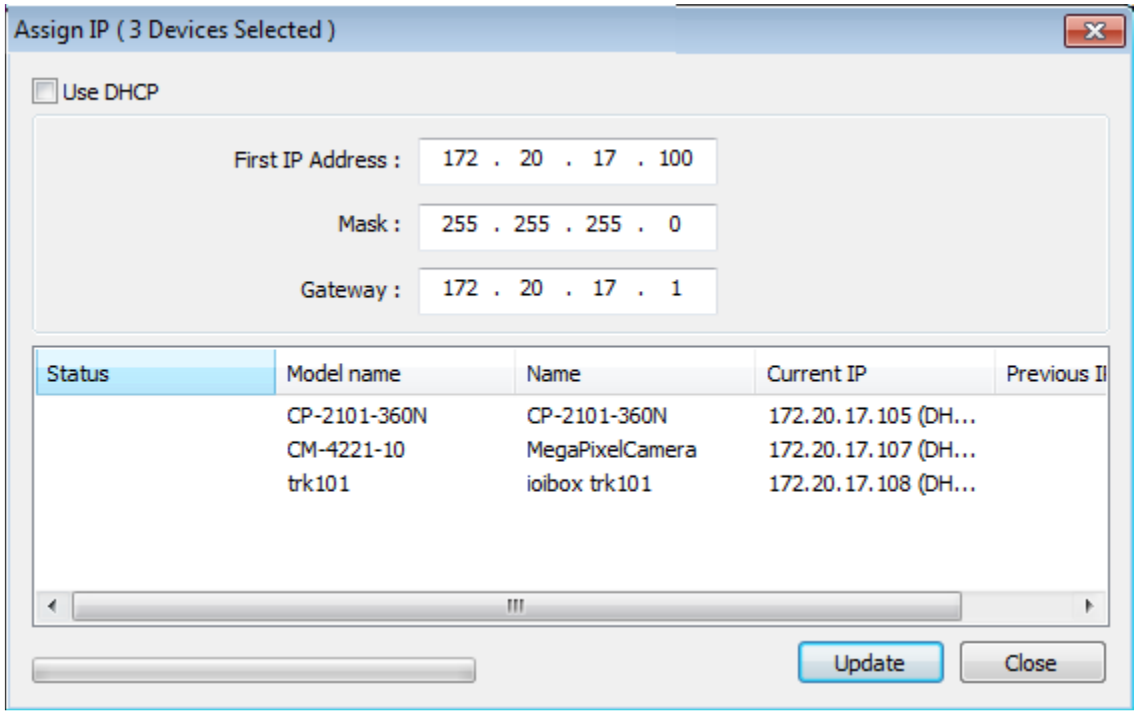
1. Select the *Use DHCP* checkbox in the **Assign IP** window. IP parameters are grayed when the *Use DHCP* checkbox is selected.
2. Click **Update**. All the selected units switch to DHCP mode and get the IP address from the DHCP server.

To manually set an IP address on multiple devices

1. Be sure that you do not check the *Use DHCP* checkbox.
2. Set the Subnet Mask.
3. Set the Gateway IP.
4. Set the *First IP address* or use the current one which is automatically set if you have already logged in before.
5. Click **Update**.

Note:

It is possible to stop this procedure by clicking **Cancel**. However, this action is not recommended.


Assign IP (3 Devices Selected)
Use DHCP
First IP Address : 172 . 20 . 17 . 100
Mask : 255 . 255 . 255 . 0
Gateway : 172 . 20 . 17 . 1
Status
Model name
Name
Current IP
Previous II
CP-2101-360N
CP-2101-360N
172.20.17.105 (DH...
CM-4221-10
MegaPixelCamera
172.20.17.107 (DH...
trk101
ioibox trk101
172.20.17.108 (DH...
Update
Close

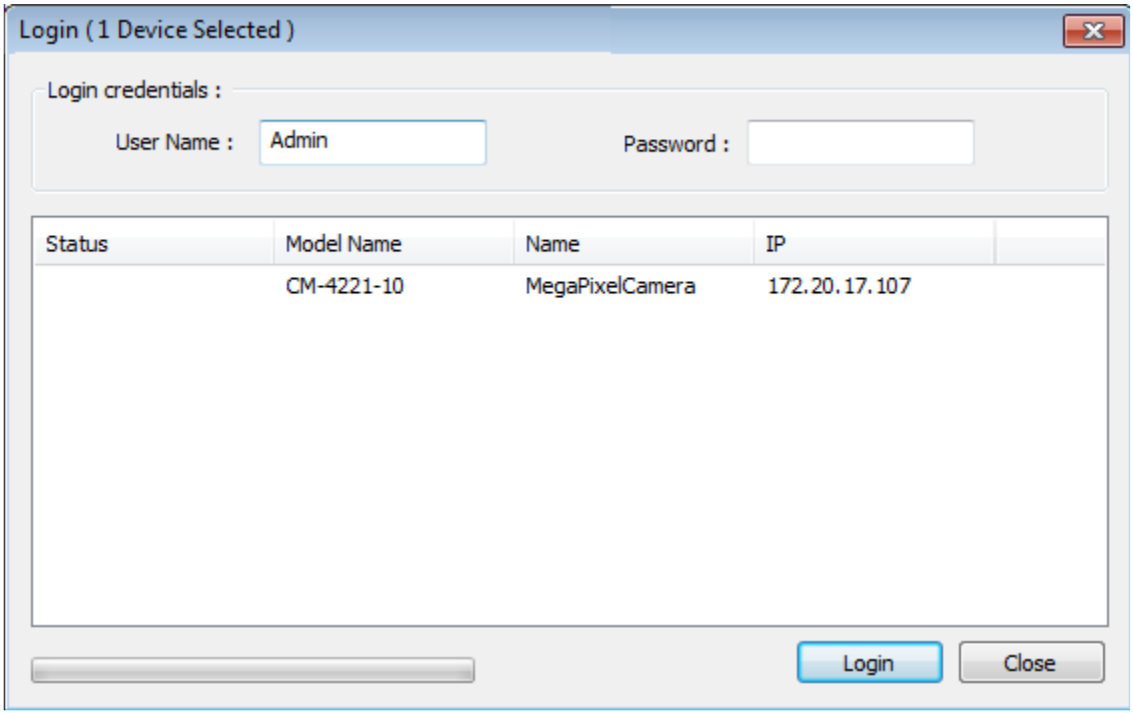
The Assign IP procedure updates all selected devices. The IP address is set automatically for each device starting from the First IP Address. The Subnet Mask and Gateway IP addresses are assigned automatically to all selected devices. If the procedure is successful, “OK” is displayed in the *Status* column.

4.1.2.2 Login Tab

The **Login** tab 

or context menu option is used to enter the user name and password (“credentials”) of a device that is not authenticated.

Selecting the **Login** tab or context menu option opens the **Login** window, which displays a list of all selected devices.



The upper area of the **Login** window displays the user name and password (login credentials) for each device. The lower area displays the status of the login operation, including the following information:

- Status
- Model Name
- Name (device name)
- IP

A Progress bar at the bottom of the window displays the progress of the login operation.

During the discovery process, DNA requests device details by using default credentials that are hard-coded in DNA. DNA tries to login with default credentials or credentials recalled from the last session. If DNA cannot login because of incorrect credentials, the device’s status is listed as “Not authenticated” in the Discover List. In this case, you must use the **Login** tab to enter login credentials.

If a device is not authenticated after discovery, login to the unauthenticated device(s).

To log into a device

1. Select the unauthenticated device(s) from the Discover List.
2. Select the **Login** tab. The **Login** window opens.
3. Enter user name and password in the **Login** window.
4. Click **Login**. DNA sends the user name and/or password to the selected devices and tries to login with these credentials.

If DNA is successful logging into the device, a green check mark is displayed to the left of the device in the **Login** window status area. The device is updated as authenticated in the Discover List.

If DNA is not successful logging into the device, a red is displayed to the left of the device in the **Login** window status area. The device remains listed as unauthenticated in the Discover List. In this event, enter a new user name and/or password.

Note:
It is possible to stop this procedure by clicking **Cancel**. However, this action is not recommended.

4.1.2.3 Web Tab

The **Web** tab or context menu option opens the web page of the selected device, which enables device configuration.

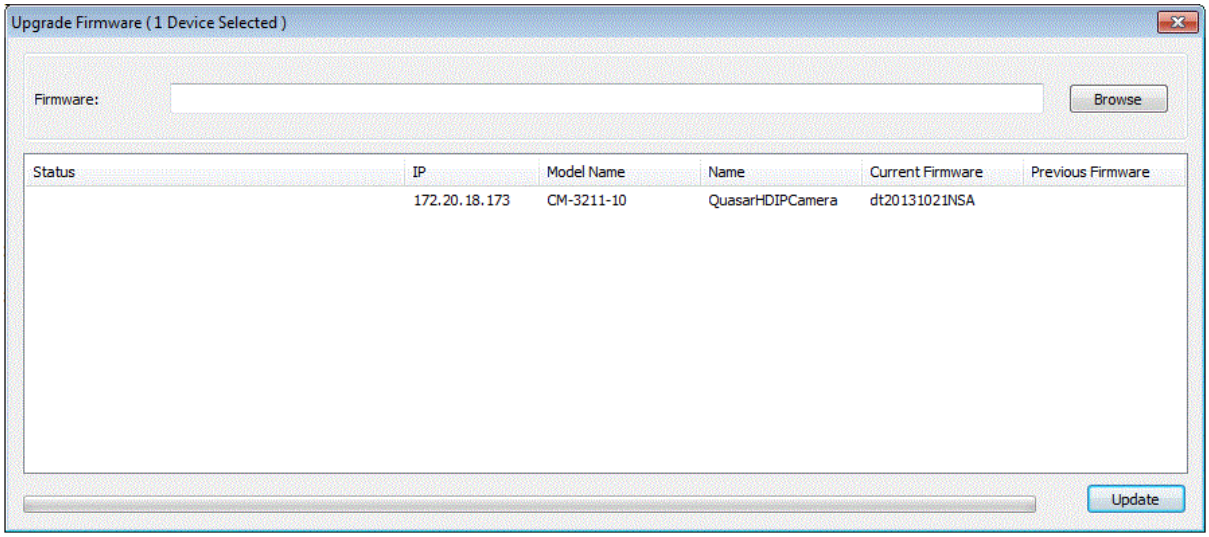
You must manually close the web browser when finished using the device's web interface. This option is not available for bulk operation.

4.1.2.4 Firmware Tab

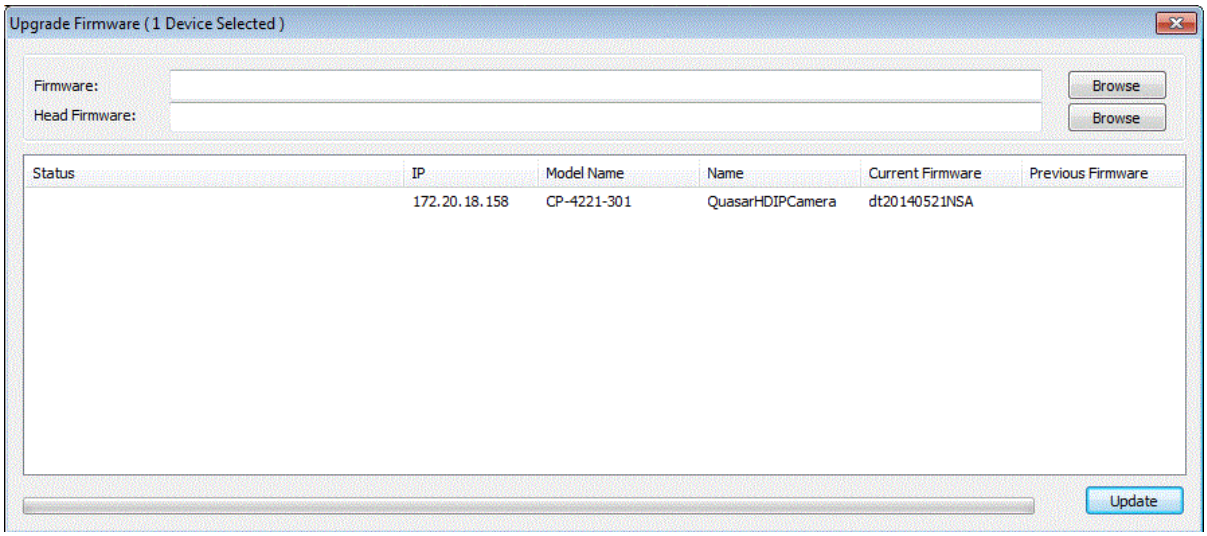
The **Firmware** tab or context menu option is used to update the firmware of one or more authenticated devices.

Caution:
A firmware update should be performed only by authorized service personnel.

After selecting the **Firmware** tab or option, the **Upgrade Firmware** window opens. The upper area displays the path for the firmware version for the camera.



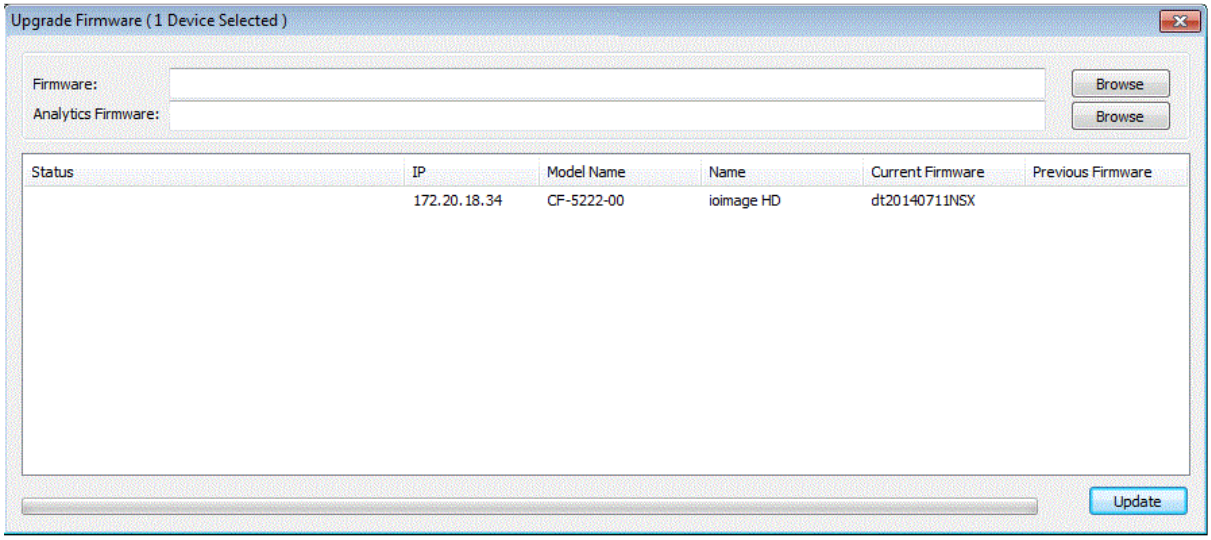
When updating the firmware for a Quasar PTZ camera, the upper area includes the path for the PTZ head firmware, in addition to the unit's firmware.



Note:

When updating the firmware of a Quasar PTZ camera from firmware version dt2012xxxxNSA to version dt2013xxxxNSA, be sure to update the PTZ head firmware and the device firmware.

When updating the firmware for an ioimage HD camera, the upper area includes the path for the camera firmware, in addition to the analytics firmware.



The lower area of the screen displays device status information, including:

- Status — Upgrade process status
- IP — Device IP address
- Model Name
- Name — Device Name
- Current Firmware — Firmware version after the upgrade
- Previous Firmware — Firmware version before the upgrade

The Progress bar at the bottom of the window displays the progress of the firmware update operation.

Note:
Because firmware is device-type dependent, the DNA application can only update authenticated devices of the same type (i.e. vendor and model) that use the same firmware.

Note:
The firmware upgrade for an ioimage Thermal camera may take up to one hour.

To update firmware

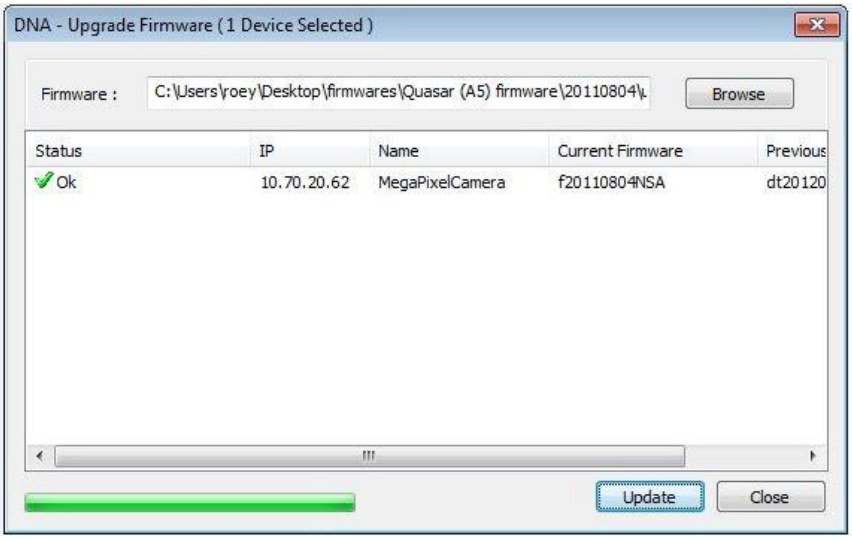
1. From the Discover List, select the device(s) to be upgraded. The Title bar of the **Upgrade Firmware** window displays the number of selected devices.
2. Click **Browse** to locate the desired firmware file.
3. Click **Update**. DNA starts to update the devices. There is no limitation to how many units can be upgraded.

Note:

1. It is recommended to update no more than 20 units at a time.
2. It is possible to stop this procedure by clicking **Cancel**. However, this action is not recommended.

If the firmware update operation is not successful, a red icon is displayed next to a message in the *Status* column.

If the firmware update is successful, a green check mark and "OK" are displayed to the left of the device in the status area of the **Upgrade Firmware**. The new firmware version appears in the *Current Firmware* column and the previous firmware version appears in the *Previous Firmware* column. The **Cancel** button is replaced by the **Update** button.



Note:

When updating the firmware of an ioimage Thermal camera, a status message "OK. The sensor firmware is upgrading." is displayed. The update process can take up to one hour, but the camera continues to function during this time.

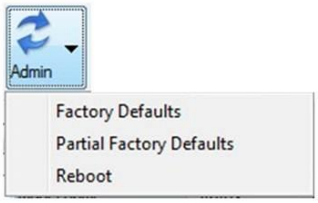
The device is updated as authenticated in the Discover List.

Caution:

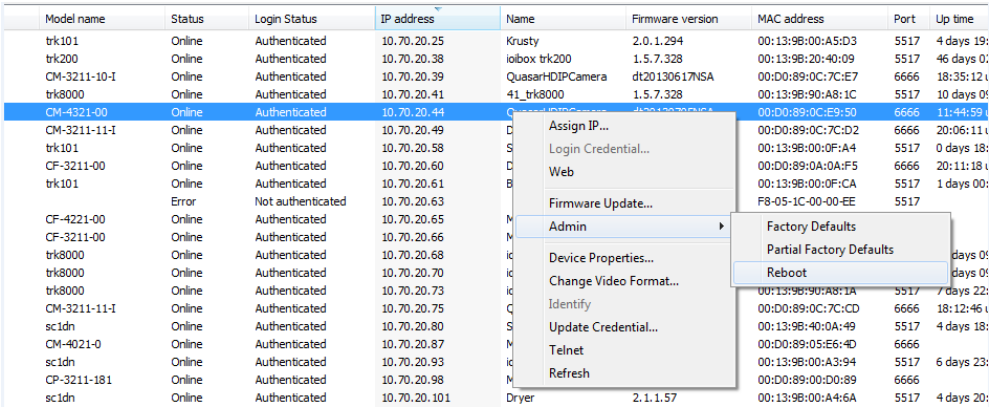
Do not exit the application while a firmware upgrade is in process.

4.1.2.5 Admin Tab

The Admin tab  or context menu option is used to select *Factory Defaults*, *Partial Factory Defaults*, or *Reboot*. Clicking on the arrow on the **Admin** tab opens the following drop-down menu:



The drop-down menu can also be accessed by right-clicking on **Admin** in the context menu:



4.1.2.5.1 Factory Defaults

Selecting the *Factory Defaults* option from the drop-down menu sets a full restore to default settings for device configurations and network properties as set in the factory. A full or partial factory default update also restores the default credentials.

The *Factory Defaults* option is enabled when:

- Only one device is selected from the Discover List
- The device is online
- The selected device is authenticated

> **Caution:**
> A batch Factory Default should be performed only by authorized service personnel.

4.1.2.5.2 Partial Factory Defaults

Selecting the *Partial Factory Defaults* option restores the device to all factory defaults, except for the network properties (i.e. IP address, etc.).

The *Partial Factory Defaults* option is enabled when:

- One or more devices are selected from the Discover List
- The devices are online
- The selected devices are authenticated

To perform single or batch Partial Factory Default

1. Select the device(s) for the partial factory default from the Discover List.
2. Select the **Admin** tab or context menu option.
3. Select *Partial Factory Defaults*. DNA performs a partial factory default on the device(s). The device reboots. A new login is performed automatically with default credentials.

4.1.2.5.3 Reboot

Selecting the *Reboot* option reboots the device.

The *Reboot* option is enabled when:

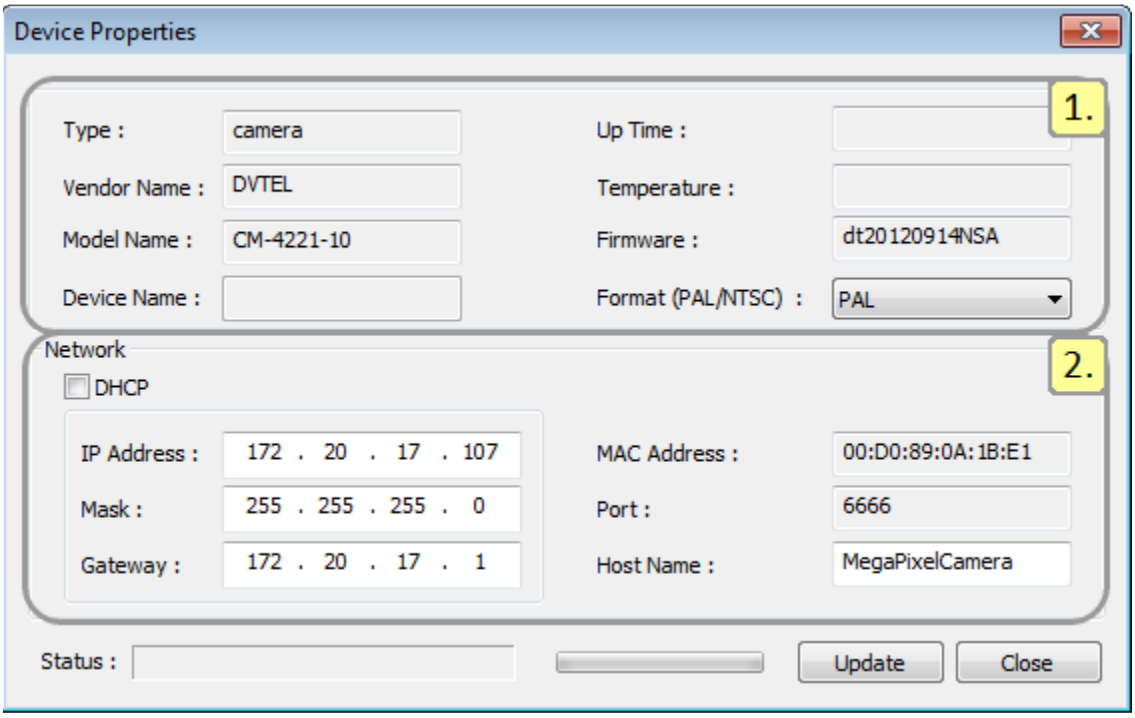
- One or more devices are selected from the Discover List
- The devices are online
- The selected devices are authenticated

To perform a single or batch reboot

1. Select the devices to reboot.
2. Select the **Admin** tab or context menu option.
3. Select **Reboot**. The devices are rebooted.

4.1.2.6 Properties Tab

The **Properties** tab  or context menu option is used to open the **Device Properties** window. The screen includes two areas: one for device details and one for network details.



The upper section of the screen displays the following device details:

- Device Type
- Vendor Name
- Model Name
- Device Name

- Up Time
- Temperature
- Firmware
- Format (PAL/NTSC)

Note:

1. Up Time, Temperature, and Format (PAL/NTSC) are automatically discovered if these parameters are available from the device. If these parameters are not available, the fields are empty and disabled (grayed out).
2. The *Format (PAL/NTSC)* field is disabled if the device is not online or if the device does not enable changing the format. In these cases, the *Format (PAL/NTSC)* field is disabled and displays *Blank*. If the device supports setting the video format, but it does not provide the value to DNA, the drop-down list displays *Blank* and is enabled.

The lower section of the screen displays network details including:

- IP Address
- Mask
- Gateway
- MAC Address
- Port
- Host Name

Note:

If an Ariel camera or encoder is not authenticated, you must first authenticate it before performing the following steps.

To set the TV system format for one unit

1. Click the **Properties** tab in the Navigation Bar or select the *Properties* option in the context menu. The **Device Properties** window opens.
2. From the *Format (PAL/NTSC)* drop-down list, select NTSC or PAL.

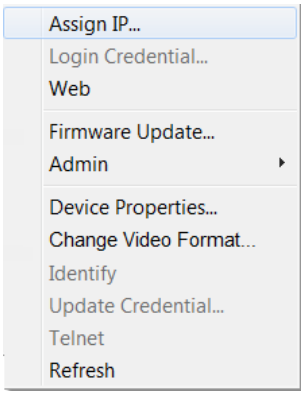
   Note:

   If the video format of an ioi unit changes, the unit is reset to factory defaults and the analytic setup is deleted. A message is displayed in the unit's web interface requesting you to approve the change.

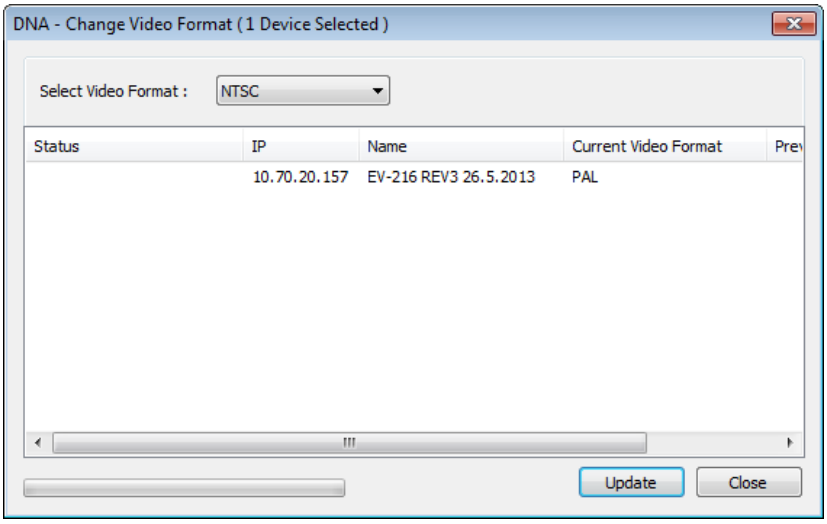
3. Click **Update**.

To set the TV system format for multiple units

1. Right-click your mouse to open the context menu. The context menu opens.



2. Select the *Change Video Format* option. The *Change Video Format* window opens.



3. From the *Video Format* drop-down list, select *NTSC* or *PAL*.
4. Click **Update**. The device reboots. While rebooting, the status of the reboot is displayed in the *Status* column. After rebooting, DNA checks if the value has been changed correctly. The dialog box displays the previous video standard and the current video standard in the respective column.

The device's properties are obtained during discovery. Available properties are dependent upon the device type. If a property is not supported by the selected device type, the property field is gray.

An offline device can be viewed; however, properties cannot be changed. The displayed device properties are from the last time the device was online.

To set the device name for a selected device

1. Click the **Properties** tab in the Navigation Bar or select the *Properties* option in the context menu. The **Device Properties** window opens.
2. Set the new device name in the *Device Name* edit box.
3. Click **Update**. The application updates all changed device settings in the selected device.

To set the host name for a selected device

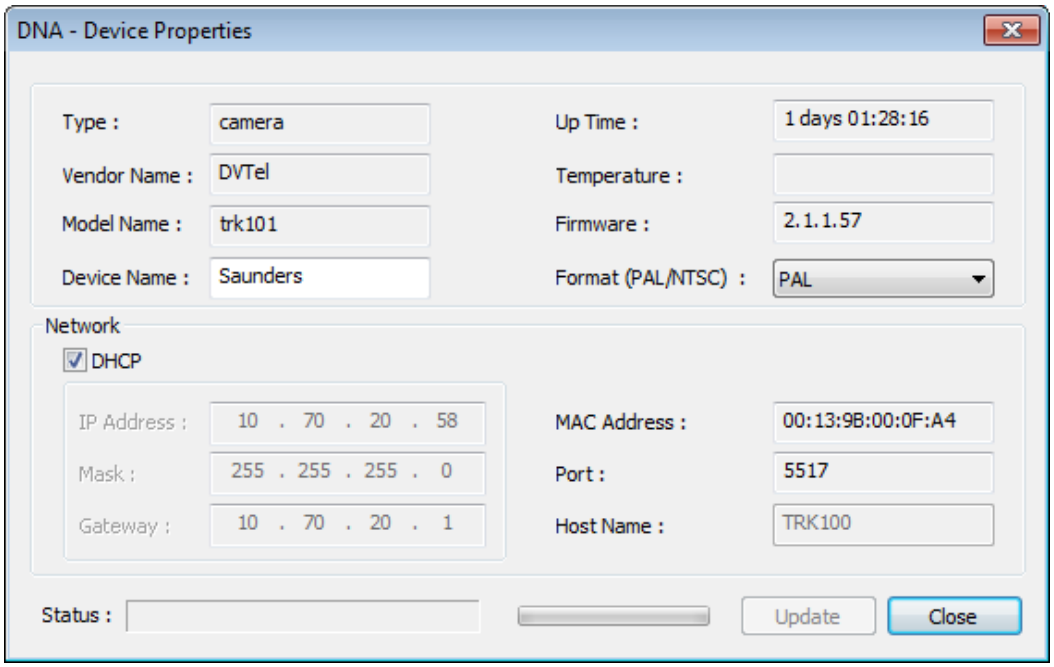
1. Click the **Properties** tab in the Navigation Bar or select the *Properties* option in the context menu. The **Device Properties** window opens.
2. Set the new host name in the *Host Name* edit box.
3. Click **Update**. The application updates all changed device settings in the selected device.

Note:

The Host Name for Quasar, HD Classic, and HD Elite cameras is displayed under the *Name* column in the Discover List, while the Device Name for DVTEL Pro Line, Pro Line A, and EV series devices is displayed under the *Name* column.

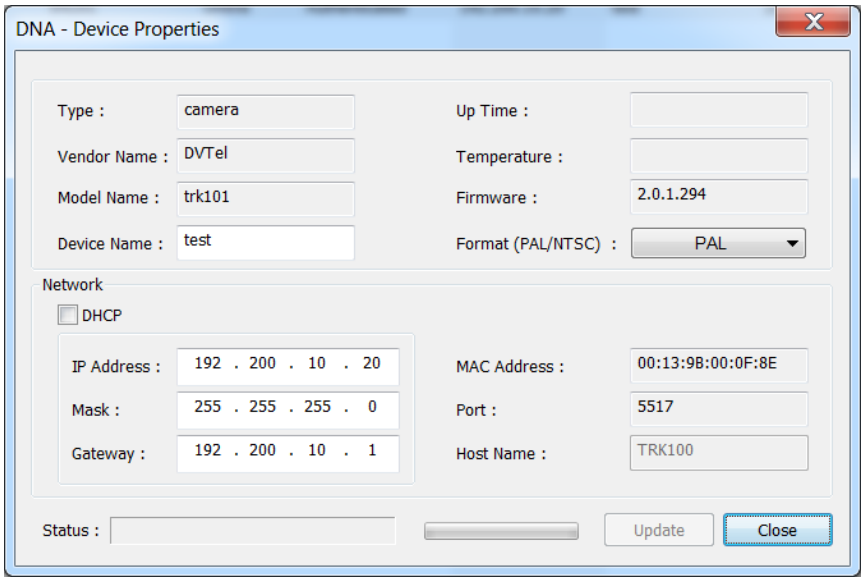
To set DHCP mode

1. Select the *DHCP* checkbox in the Device Properties window.
2. Click **Update**. The IP address, Subnet Mask and Gateway are set automatically by the DHCP server.



To manually set an IP address

1. Be sure that you do not select the *DHCP* checkbox.
2. Set the IP address.
3. Set the Subnet Mask.
4. Set the Gateway IP.
5. Click **Update**.



The **Update** button is gray if no properties are changed. As soon as a property is changed, the button becomes active. If the IP address is already used, the message "IP already used" appears in the *Status* field of the **Device Properties** dialog box.

Note:

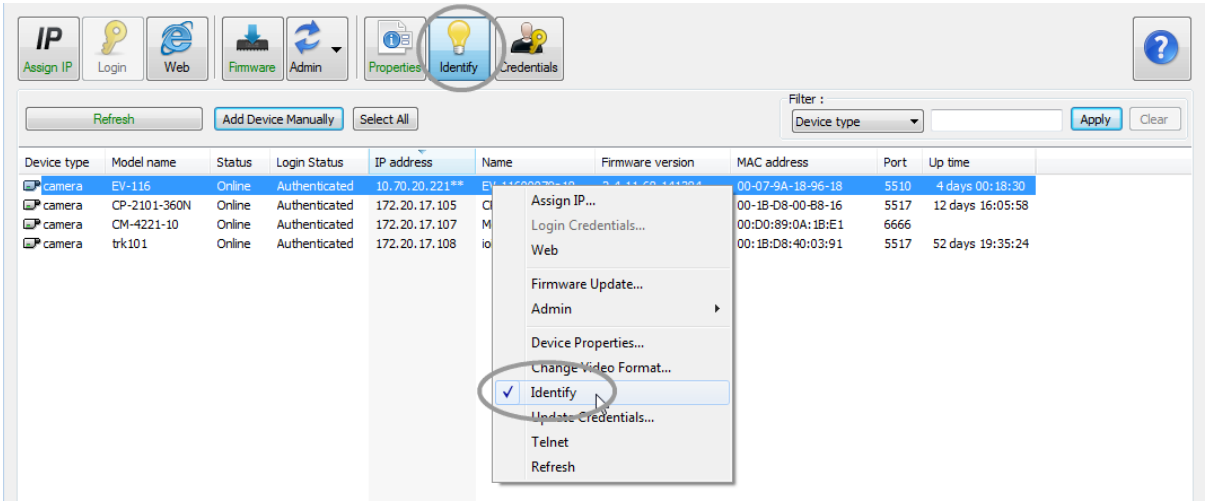
Use a unique IP address for each device.

4.1.2.7 Identify Tab

The **Identify** tab or context menu option is used to identify a selected device. Clicking this tab sends a command to the device, which turns on a physical indicator, such as an LED. When not in use, the **Identify** tab is gray.

When the **Identify** button is activated, it turns blue and remains blue as long as this function is activated. The button must be pushed again in order to deactivate it and to return the **Identify** status for the device to "off" or "not identified" mode.

The **Identify** option on the context menu displays a check mark  next to it when this option is selected, as appears here in the Discover List:



The Identify function is enabled when:

- Only one device is selected from the Discover List
- The device is online
- The device type supports this command
- The selected device is authenticated

> **Note:**
> EA and EV series devices do not support this command.

To activate the Identify function

1. Select the device(s).
2. Select the **Identify** tab or context menu option. The **Identify** tab turns blue and the *Identify* context menu option is preceded by a check mark. A LED is activated on the device(s).
3. To deactivate this function, select the **Identify** tab or right-click *Identify*.

4.1.2.8 Credentials Tab

The **Credentials** tab 

or *Update Credentials* context menu option is used for editing the device's user name and/or password ("credentials") in one or more devices after the device is already logged in.

Selecting the **Credentials** tab or context menu option opens the **Update Credentials** window, which displays a list of the selected devices to be updated. The upper area of the **Update Credentials** window displays the user name and password (login credentials) for each device. The lower area displays the status of the change credential operation, and includes the following information:

- Status
- Name (device name)
- IP

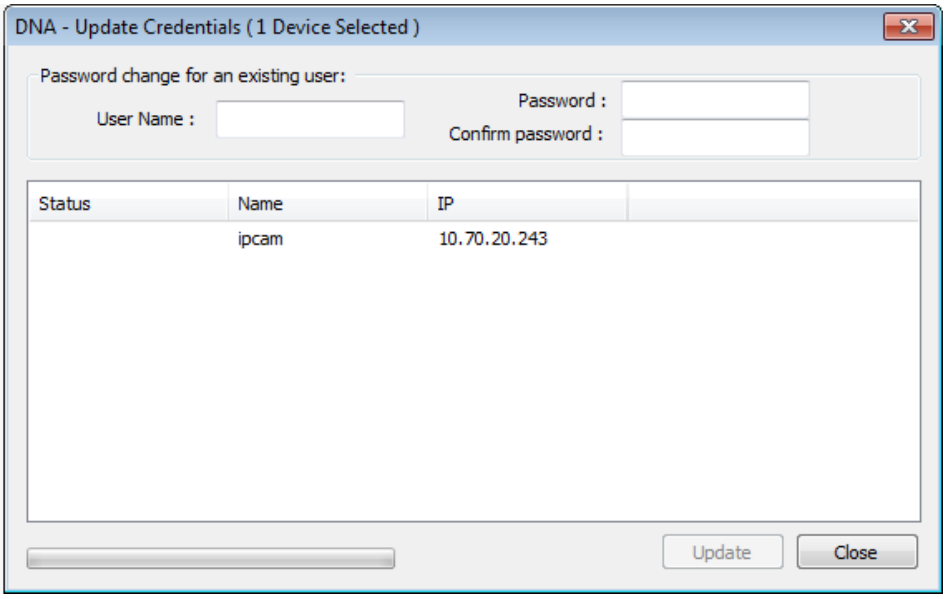
The title bar of the **Update Credentials** window displays the number of selected devices. After changing the credential, the application updates the authentication status.

To set credentials

1. Select a device or multiple devices from the Discover List.
2. Select the **Credentials** tab in the Navigation Bar or select the *Update Credentials* context menu option by right-clicking the mouse. The **Update Credentials** window opens.
3. Enter the user name and/or password in the corresponding edit box.
4. Re-enter the password in the *Confirm Password* edit box.
5. Click **Update**. DNA sends the new user name and/or password to the selected devices and tries to login with these credentials. If DNA is successful logging into the device, a green check mark and "OK" are displayed to the left of the device in the **Update Credentials** window status area. The device is updated as authenticated in the Discover List.

> **Note:**
> It is possible to stop this procedure by clicking **Cancel**. However, this action is not recommended.

The progress of the update is displayed in the Progress bar.



> **Note:**
> All credentials, except default administrator credentials, are lost when you restart the application.

The **Credentials** tab and *Update Credentials* option in the context menu are gray (disabled) if a device is not selected.

In case the password is lost or forgotten, it is possible to perform a partial restore to factory defaults, which restores the original password. See Partial Factory Defaults (page 19).

> **Note:**
> DVTEL Quasar, HD Classic, and HD Elite cameras do not support changing the user name.

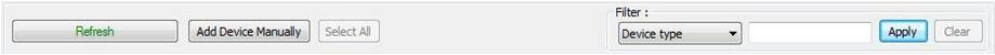
4.1.2.9 Help Button

Click **Help** for information how to use the DNA tool.

4.2 Operational Toolbar

The Operational Toolbar includes the following functions, as seen in the illustration below:

- Refresh
- Add Device Manually
- Select All
- Filter



4.2.1 Refresh

The **Refresh** button clears the Discover List and starts the discovery mechanism for all devices in the Discover List.

The *Refresh* option from the context menu starts the discovery mechanism for devices that are selected from the Discover List.

The application uses the last credentials that were used for authentication before the refresh operation.

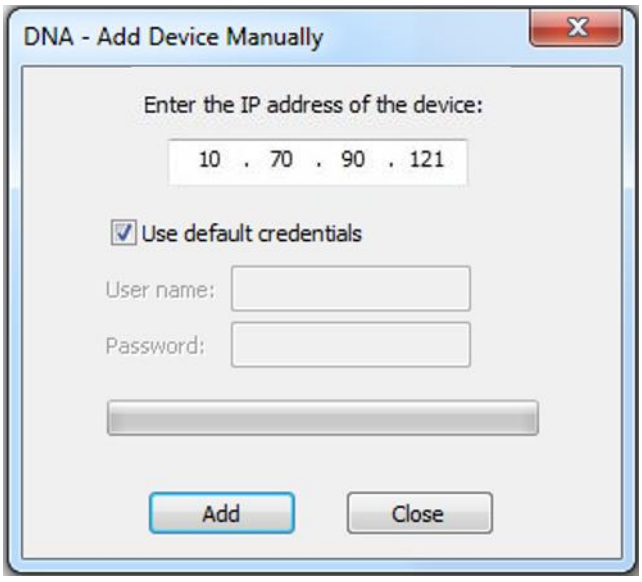
In the event of a full or partial factory default update, DNA returns to the default credentials.

4.2.2 Add Device Manually

If a device is located on a different VLAN, the device is not automatically detected. In this case, the Add Device Manually function is used to manually add the device to the Discover List.

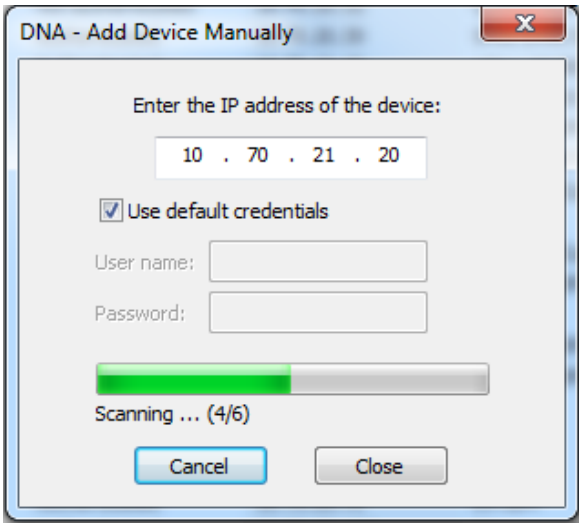
To add a device manually

1. Click **Add Device Manually** on the Operational Toolbar. The **Add Device Manually** window opens.

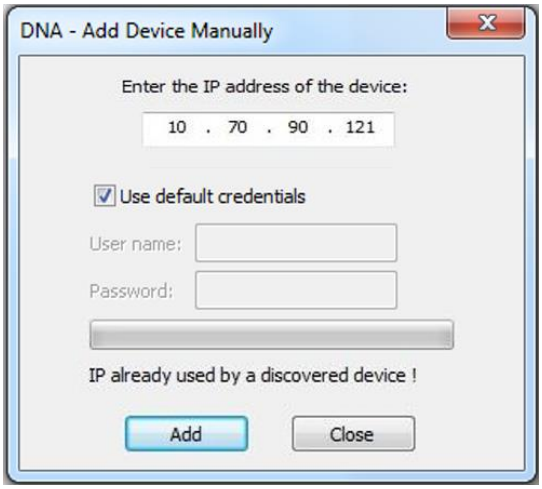


2. Enter the device's IP address.
3. Click **Add**. DNA sends the IP address to the device.

4. Status messages are displayed under the Progress bar, as illustrated below:



5. The application tries to log into the device. The added device is displayed on the Discover List and its IP address is added within double asterisks (**IP address**). When the device is discovered, the “Device found” message is displayed.
6. If the device’s IP address is already in the list, the following message is displayed:

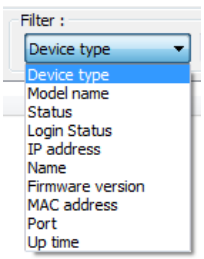


4.2.3 Select All

The **Select All** button is used to select all devices in the Discover List for a desired action, such as filtering. A reduced range can be selected by pointing the cursor to the right of the port column and selecting the desired devices.

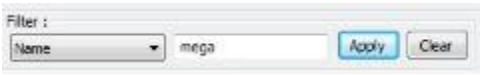
4.2.4 Filter

Clicking the **Filter** button opens the following drop-down menu:



To use the filter

1. Select the desired field to display from the drop-down menu.
2. Enter the parameter for the field you wish to filter in the edit box to the right of the filter options. You do not need to enter a complete name or number. For example, if the selected filter column is *Name* and the filter value is *MegaPixel_1 camera*, if you enter “mega” in the filter edit box, all MegaPixel cameras are displayed.



3. Click **Apply** to update the Discover List according to the filter parameter. The results for this operation are displayed in the Discover List.
4. To disable the filter, click **Clear**. The full Discover List is restored. The **Clear** button is disabled when there is no active filter.

4.3 Discover List

The Discover List displays information retrieved during the discovery operation. It includes the following columns:

- Device type (camera/encoder)
- Model name (product model name)
- Status (online/offline/error)
- Login Status (password authenticated/not authenticated)
- IP address
- Name (host name or device name)
- Firmware version
- MAC address
- Port (where applicable)

It is possible to sort the Discover List by clicking on the desired column name on the list. Clicking a second time changes the sort order (ascending/descending).

If a device goes offline, the word “offline” in the *Status* column for the device appears within angle brackets (<offline>). In order to remove the offline device from the Discover List, perform a refresh operation. The device will reappear on the Discover List without the signs.

Note:

For Quasar, HD Classic, and HD Elite cameras, the *Name* column displays the Host Name.

For DVTEL Pro Line, Pro Line A, and EV series devices, the *Name* column displays the Device Name.

4.4 Status Bar

The Status bar displays the number of discovered devices.

5 Log Files

DNA supports the creation of log files. By default, the log file is enabled. It is found in the same directory as the `DNA.exe` file.

Contacting DVTEL

To contact us, write us at info@dvtel.com or contact your local office.

CORPORATE HEADQUARTERS **DVTEL, Inc.** 65 Challenger Road Ridgefield Park, NJ 07660 USA Tel: 201.368.9700 Fax: 201.368.2615 Order Fax: 201.712.0343 info@dvtel.com	**ASIA PACIFIC REGION** **DVTEL** 111 North Bridge Road, #27-01 Peninsula Plaza Singapore 079098 Tel: +65 6389 1815 Fax: +65 6491 5660 info.apac@dvtel.com
ANZ AND THE PACIFIC ISLANDS **DVTEL** 37 Victoria Street Henley Beach, SA 5022 Australia Tel: +61 8 8235 9211 Fax: +61 8 8235 9255 Mobile: +61 419 850 166 info.anz@dvtel.com	**EMEA** **DVTEL UK Ltd.** 7 Lancaster Court, Coronation Road High Wycombe HP12 3TD England Tel: +44 (0) 1494 430240 Fax: +44 (0) 1494 446928 info.uk@dvtel.com
INDIA AND SAARC, GULF REGION **DVTEL India Pvt., Ltd**. 303, SSR Corporate Park Mathura Road Faridabad 121002 Haryana, India Tel: +91 (129) 431 5031 Fax: +91 (129) 431 5033 info.asia@dvtel.com	**CENTRAL AND LATIN AMERICA** **DVTEL Mexico S.A.P.I. de C.V.** Felipe Villanueva No. 10 Col. Guadalupe Inn México, D.F. 01020 México Tel: +5255 5580 5618 Fax: +52 55 8503 4299 info.cala@dvtel.com
DVTEL NORTH ASIA 2404, 24/F, World-Wide House 19 Des Voeux Road Central Hong Kong Tel: +852 3667 9295 Mobile: +852 9479 4195 info.northasia@dvtel.com	**DVTEL北亞地區** 香港中環德輔道中19號 環球大廈2404室 電話: +852 3667 9295 手提: +852 9479 4195 電郵: info.northasia@dvtel.com

To request the latest versions of firmware and software or to download other product-related documents, visit http://www.dvtel.com/support. If you have obtained a login, go to our support gateway. For assistance, email us at support@dvtel.com or phone 1-888-DVTEL77.