



Installation Guide - SureStream

Vega Systems Inc.,
1999 S Bascom Ave #700,
Campbell, CA 95008
USA
info@vega25.com

Table of Contents

Table of Contents	1
Version Information	2
Introduction	2
First-time Installation	2
Obtaining Software	2
Install Software	2
Onvif tools installation	2
Plug-In Installation - Management Server	3
Plug-In Installation - Smart Client	8
Prerequisites - Server Specification	8
Offline License Activation	12
Online License Activation	12
Step1: Provide SLC	12
Step 2: Activate	13
Upgrading Software	17
Un-Installation	17
Things to check before running software	21
Step 1: Date and Time Sync in Camera and Smart Client Machines	21
Step 2: WiFi Disable in the Smart Client Machine.	24
Step 3: Virtual Machine Adapter Disable in Smart Client Machine	28
Step 4: Replay attack mode should be off in camera (specifically for Axis camera)	32
Contact Us	36

Version Information

Version #	Date	Changes
1.0	May-2018	Software Release 3.0
2.0	Sep-2018	Software Release 4.0.3
3.0	Oct 2018	Updated troubleshooting guide

Introduction

SureStream is a MIP Plugin solution that enables direct multicast from the camera to the SmartClient. Recording/Management server failures have no effect on it.

First-time Installation

Please follow the steps listed below to obtain and install SureStream.

Obtaining Software

1. Please email sales@vega25.com and provide information about your requirements, including,
 - a. The number of channels you need SureStream for.
 - b. Your version of Milestone Corporate, Expert, Professional+ or Professional.
 - i. SureStream is not tested on other versions, but there is high chance that it will work.
2. Receive a quote.
3. Pay.
4. Receive a link to download the installer.
5. Download installation files.

Install Software

Please follow the below steps to install software.

Onvif tools installation

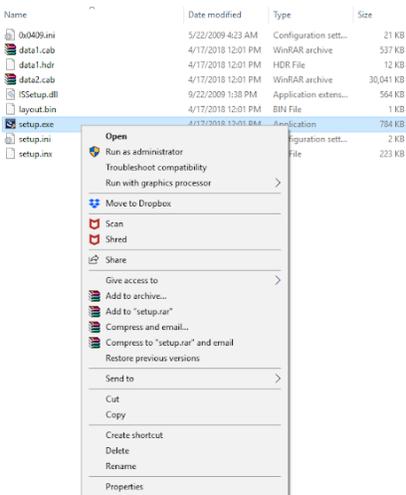
Onvif tools are not needed for SureStream, but good to have, to check onvif compatibility and to add onvif profiles.

After successful installation of SureStream, the Onvif Device Test Tool setup is present in the below path. The user can run the setup's to install.

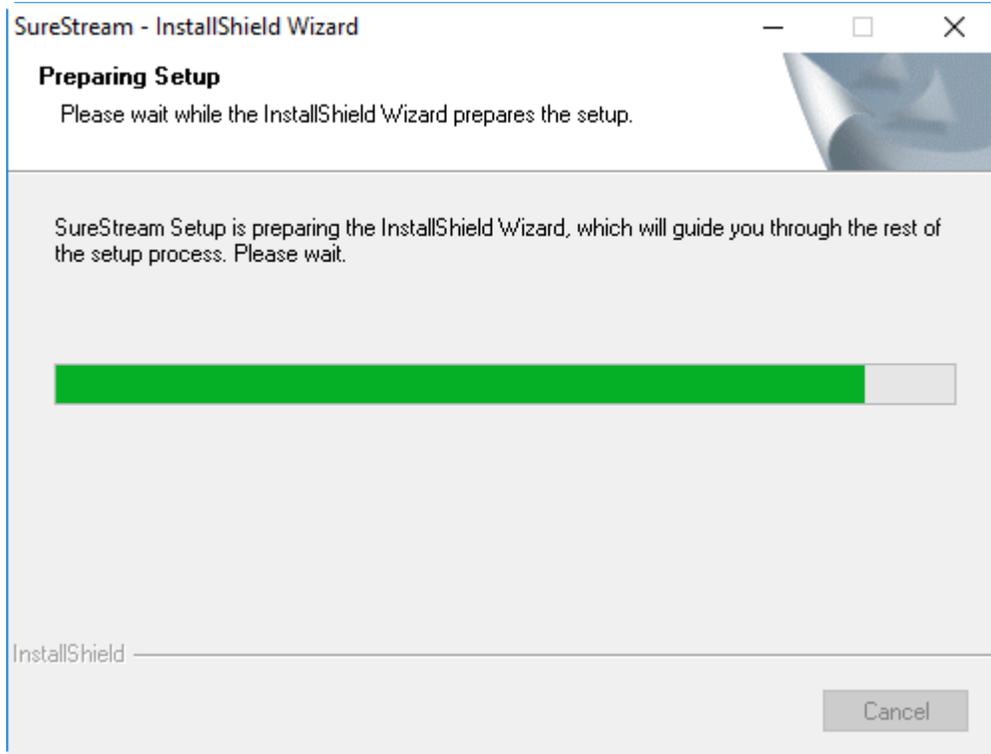
“C:\Program Files (x86)\Milestone\MIPPlugins\SureStream contains installers for Onvif Device Manager and Onvif Device Test Tool.”

Plug-In Installation - Management Server

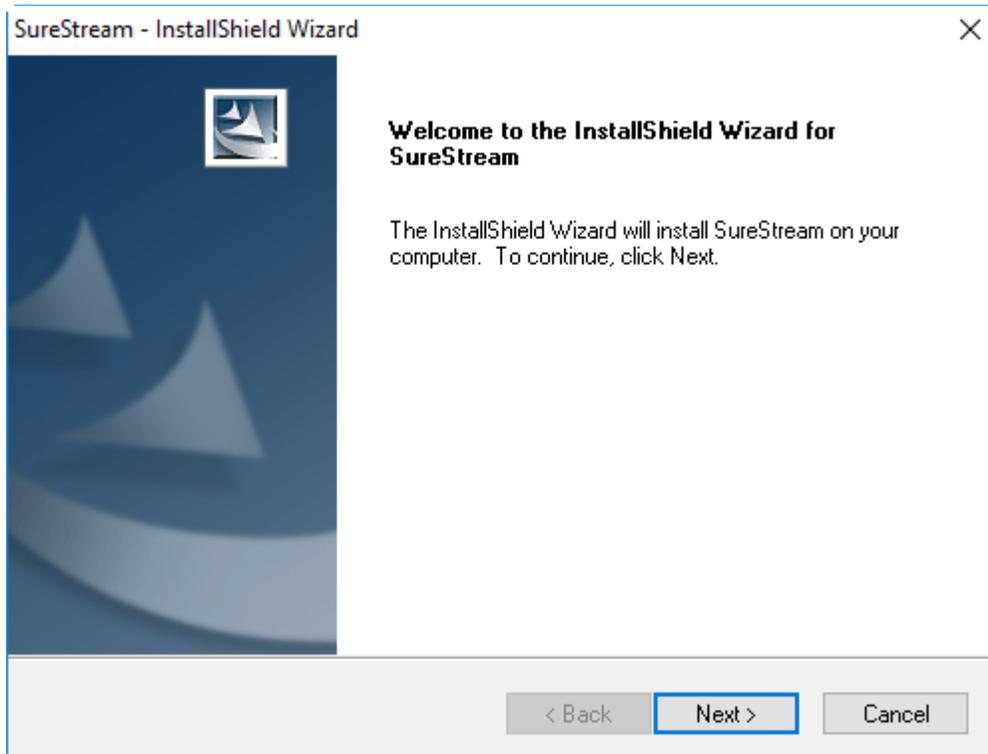
1. If your Milestone software is active on the Management Server, please follow the shutdown procedure provided by Milestone, to stop all Milestone programs running on the Milestone Management Server.
2. Copy the setup **“SureStream Setup Folder”** to a convenient location on the Milestone Management Server.
3. Open the **“SureStream Setup Folder”**, right click on the setup and click **“Run as administrator”**.



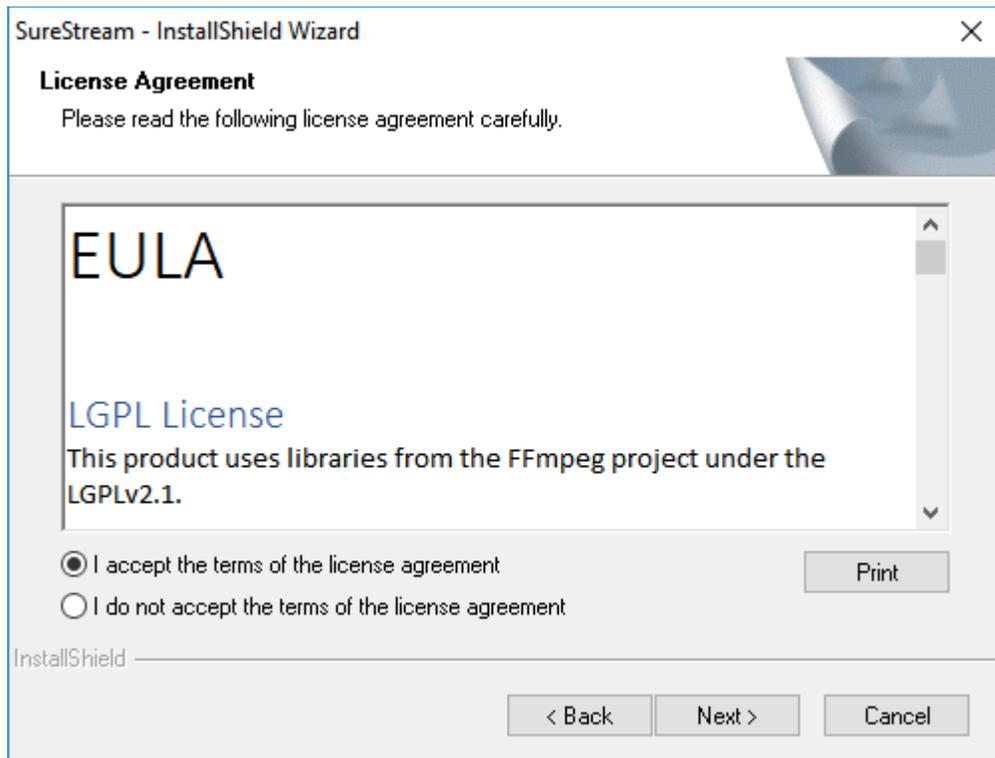
3. Upon clicking on **“Run as administrator”**, a **“Preparing to install”** window will appear as shown in the below image.



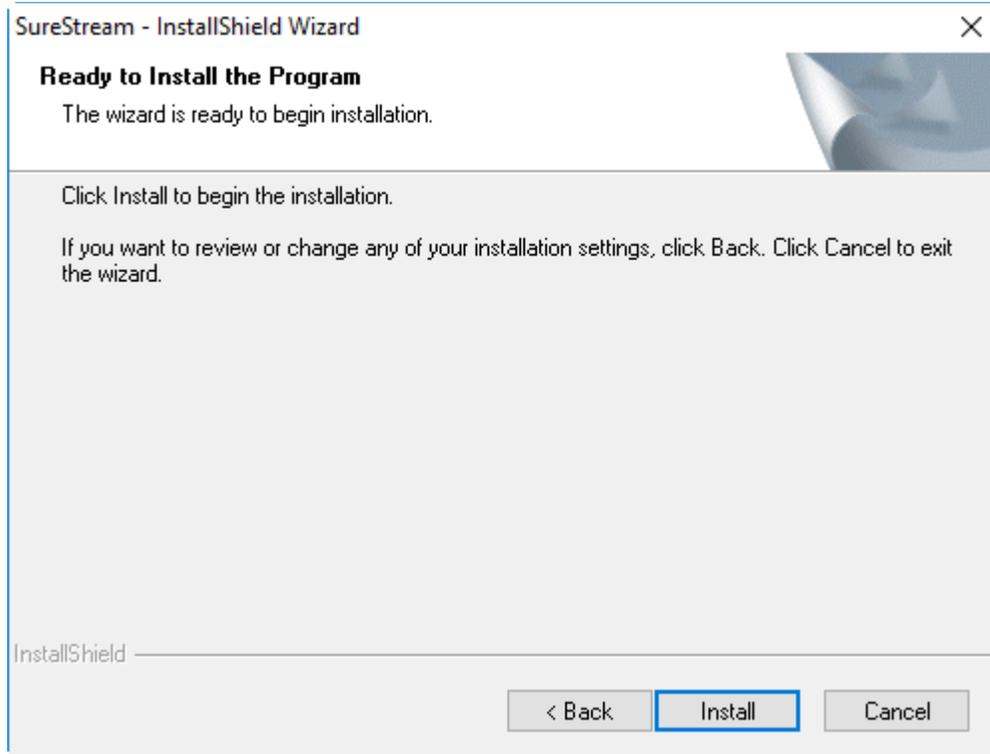
4. Once preparation is completed, the window shown below will appear. Click on the **“Next”** button.



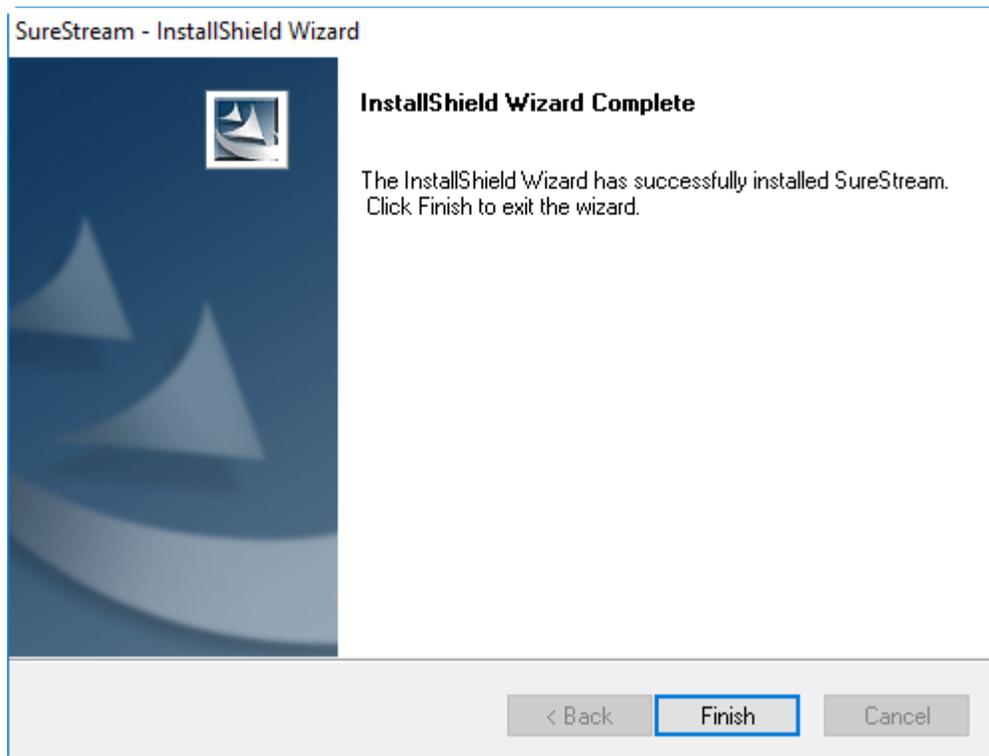
5. Upon clicking on the “**Next**” button a EULA window will pop-up.



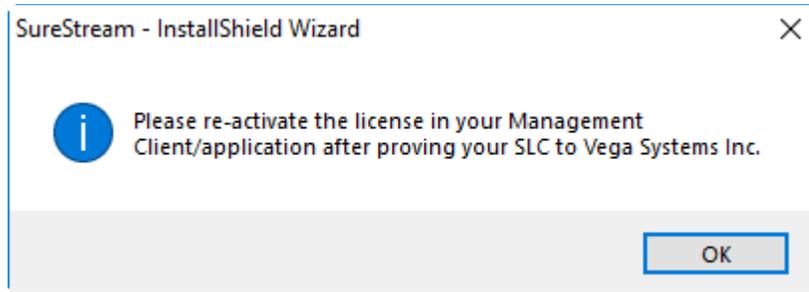
6. Select “*I accept the terms of the license agreement*” option and click on “**Next**” button.
7. Click on the “**Install**” button.



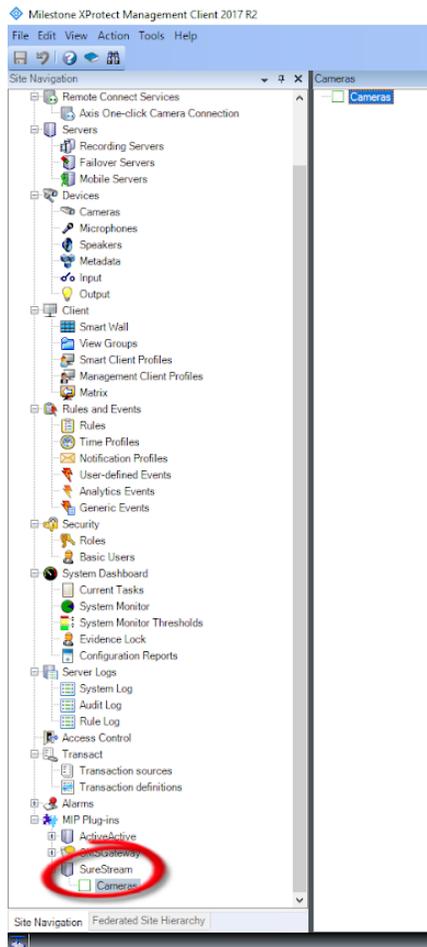
6. Upon successful Installation, the window shown below will appear.



7. After clicking "Finish", the window shown below will appear, reminding you to activate the license to begin use. Click Ok.



8. Start the Milestone Management Server. Open the Management client application.
9. Login to Management Client.
10. The newly installed plugin will show under the **MIP Plugin** tree in the Management Client application as show in the below image.



Plug-In Installation - Smart Client

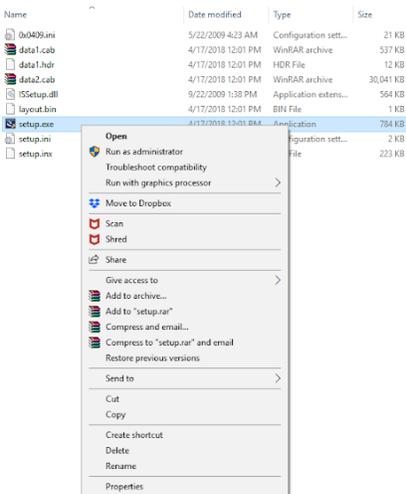
Prerequisites - Server Specification

Smart Client machine should have a minimum requirement as mentioned below

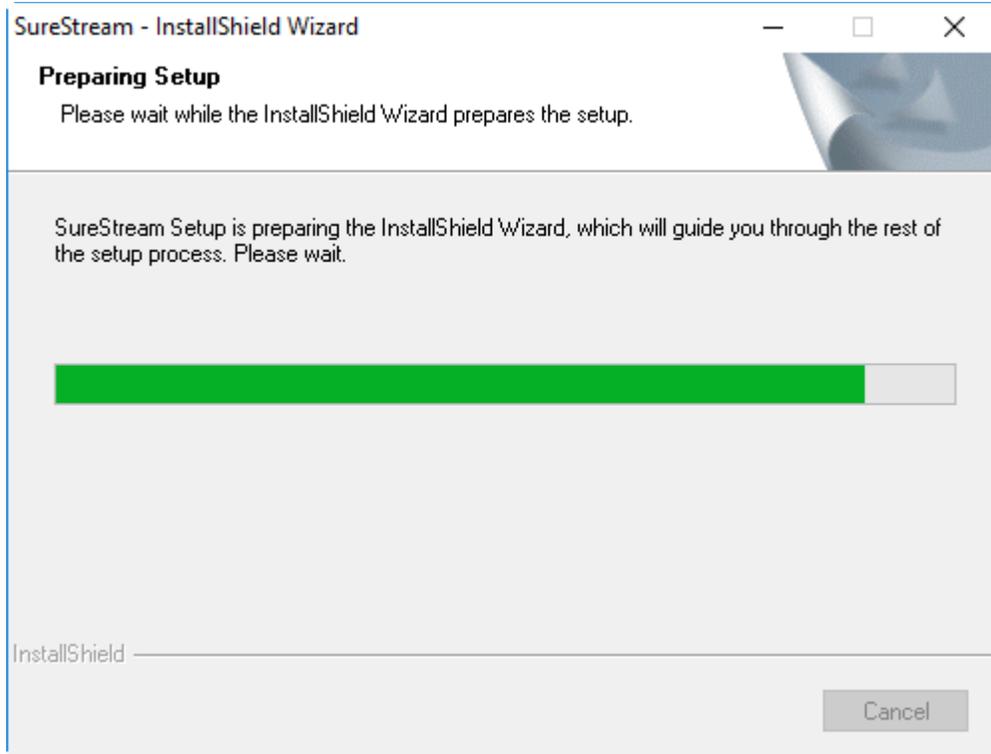
- *Processor - i5 or greater than i5.*
- *RAM- 8GB*
- *OS - 64 bit Windows 10.*
- *Use of GPU hardware acceleration for running the Smart Client is recommended.*

Follow the below procedure to install the plugin in each Smart Client machine.

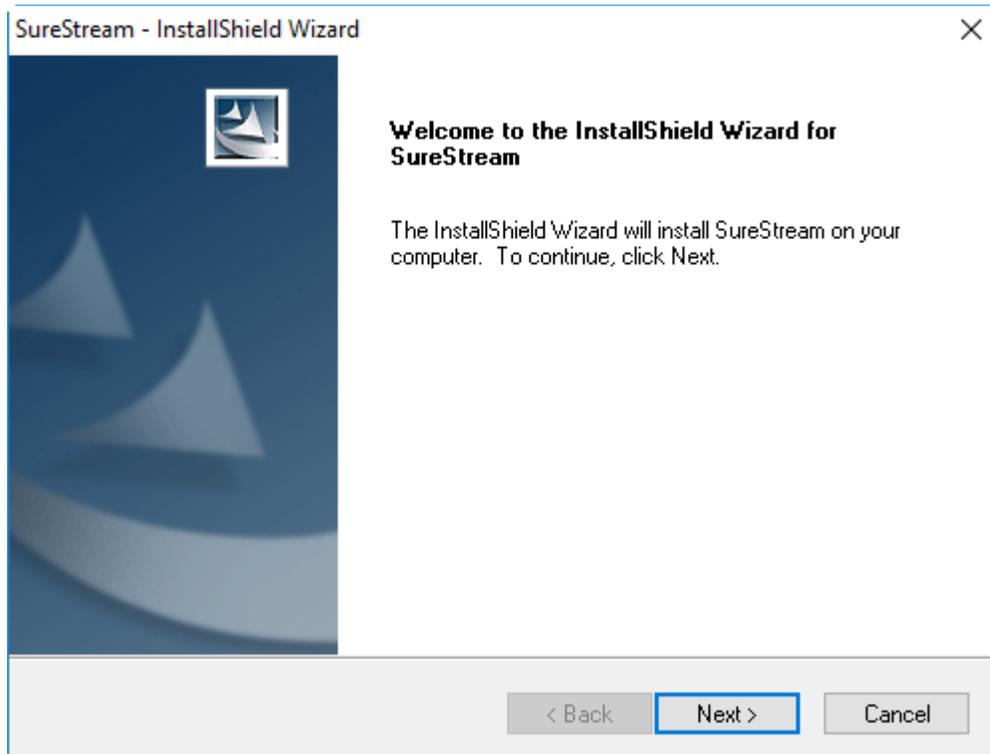
1. Close the Smart Client application if running.
2. Copy the setup **“SureStream Setup Folder”** to Milestone Smart Client machine.
3. Open the **“SureStream Folder”**, right click on the setup and click **“Run as administrator”**.



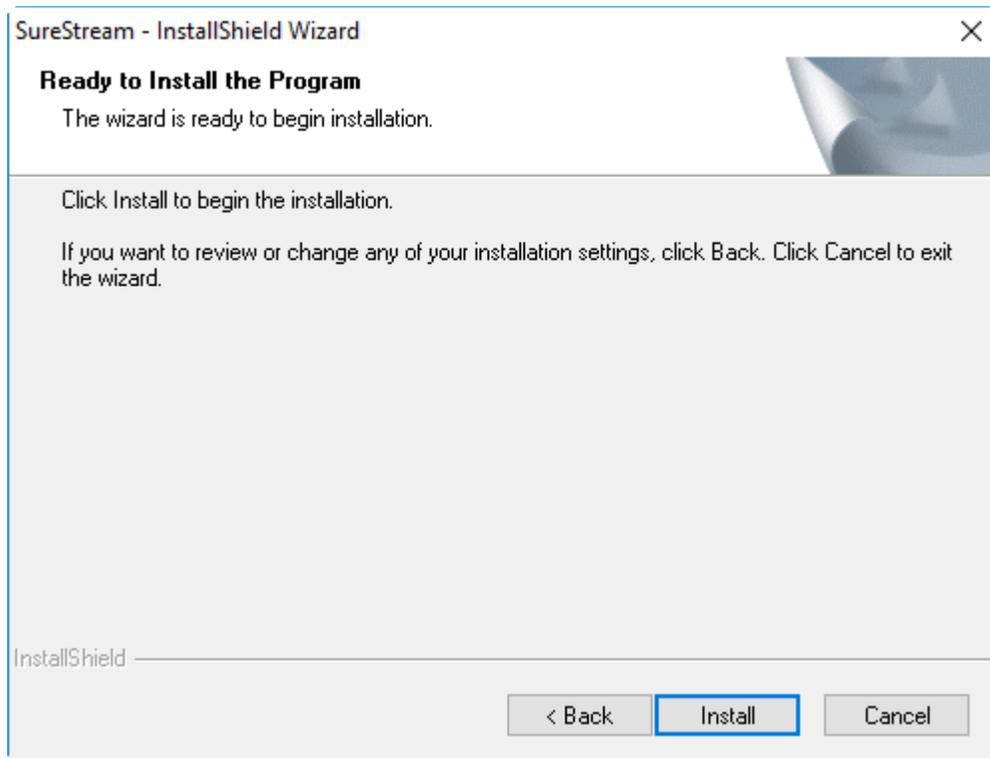
4. The **“Preparing to Install”** window will appear as shown in the below image.



5. Once preparation is completed, the window shown will appear.

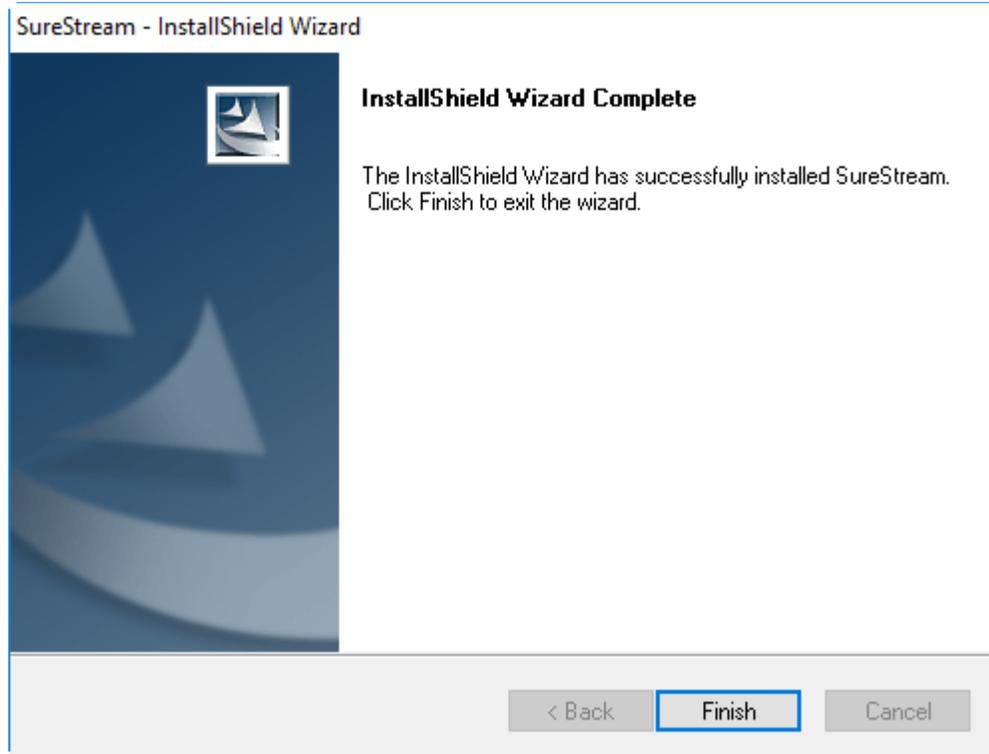


8. Click on the “**Next**” button. The window shown below will appear.

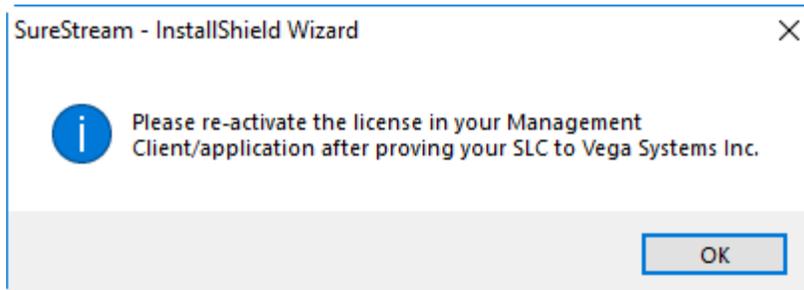


11. Click on the “**Install**” button.

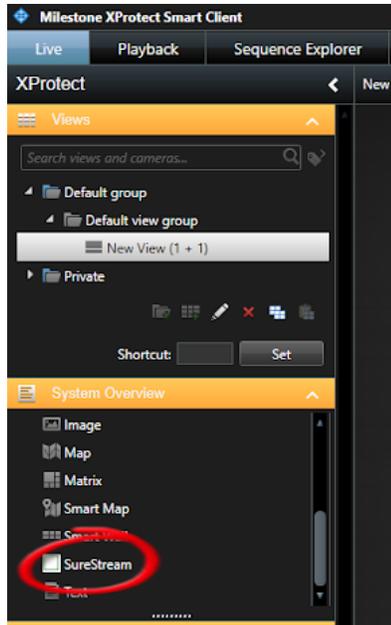
12. Upon successful Installation, we see:



13. Click on the “**Finish**” button to complete the installation.
14. Upon clicking the “**Finish**” button, you will be reminded to activate the license. Please follow steps in the next section to activate the license. Click OK.



19. Open Smart Client on the machine on which the plugin was installed.
20. The newly installed plugin will appear under the **MIP SDK Tools tree** in the Smart Client application as shown in the below image.



Offline License Activation

Read the 'Offline Activation for Plugin Licensing' document.

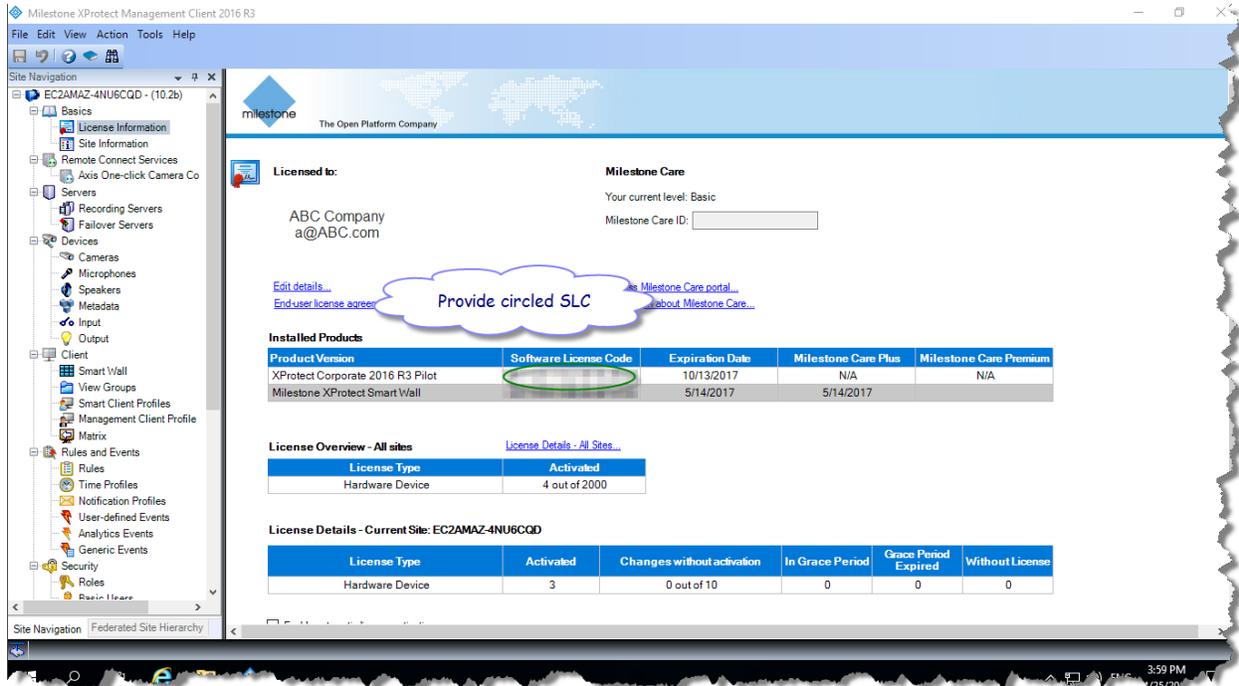
Online License Activation

This is a two-stage process as described below.

If you provided the SLC of your XProtect prior to installation and Vega confirmed licensing, proceed directly to Step 2.

Step1: Provide SLC

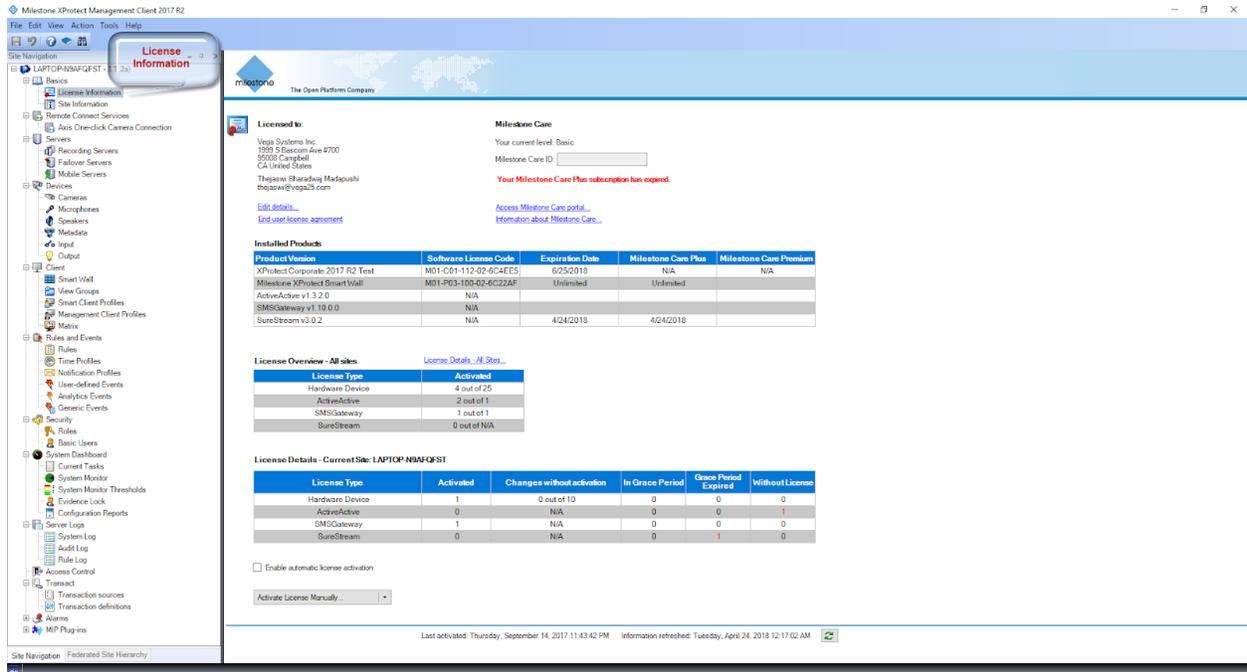
1. Provide your Xprotect Corporate SLC (Software License Code) to Sales@vega25.com. This is shown in the screenshot below.
2. Wait for an email from Vega, confirming the activation of license.
3. Proceed to Step 2.



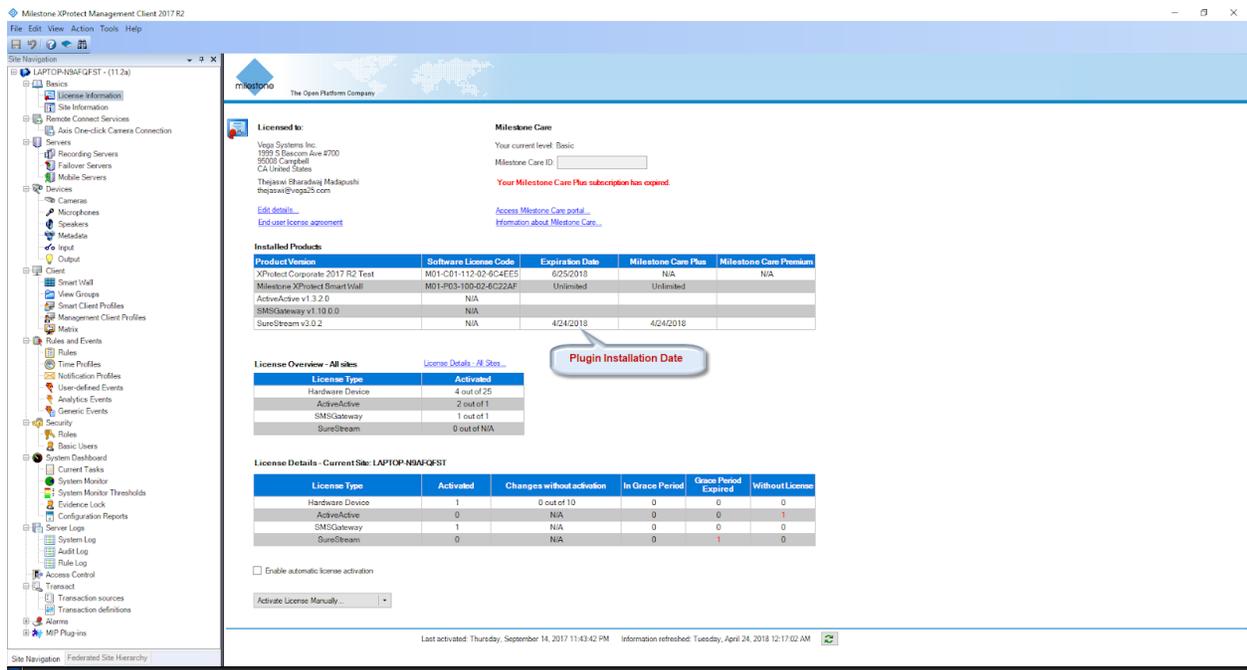
Step 2: Activate

Please follow the below procedure to activate the license.

1. This process needs your XProtect installation to be able to access the internet. Please check internet connectivity before doing the steps below.
2. After Login to Management, Client click on the **License Information** tab.



3. Upon Clicking on License Information, the below window will appear and show that the SureStream plugin has expired (It shows the expiration date as Plugin Installation Date).



4. Click on the **Activate License Manually** button.

The screenshot shows the Milestone XProtect Management Client 2017 R2 interface. The left sidebar contains a navigation tree with categories like Site Information, Servers, Devices, Client, Rules and Events, Security, System Dashboard, and Transact. The main content area displays license information for site LAPTOP-NBAFGFST-11.2a. It includes sections for 'Licensed to' (Vega Systems Inc.), 'Milestone Care' (Basic), and 'Installed Products' (XProtect Corporate 2017 R2 Test, Milestone XProtect SmartWall, ActiveActive v1.3.2.0, SMSGateway v1.10.0.0, SureStream v2.0.2). Below these are two tables: 'License Overview - All sites' and 'License Details - Current Site: LAPTOP-NBAFGFST'. The 'Activate License Button' is highlighted with a red circle and a callout box.

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 2017 R2 Test	MD1-C01-112-02-6C4EE5	6/25/2018	N/A	N/A
Milestone XProtect SmartWall	MD1-P03-100-02-6C22AF	Unlimited	Unlimited	
ActiveActive v1.3.2.0	N/A			
SMSGateway v1.10.0.0	N/A			
SureStream v2.0.2	N/A	4/24/2018	4/24/2018	

License Type	Activated
Hardware Device	4 out of 25
ActiveActive	2 out of 1
SMSGateway	1 out of 1
SureStream	0 out of N/A

License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Hardware Device	1	0 out of 10	0	0	0
ActiveActive	0	N/A	0	0	1
SMSGateway	1	N/A	0	0	0
SureStream	0	N/A	0	1	0

5. Upon clicking on the **Activate License Button** Online / Offline activation option will pop down.

This screenshot is similar to the previous one, but the 'Activate License Manually...' dropdown menu is open, showing 'Online' and 'Offline' options. A red circle highlights the 'Online' option, and a callout box points to it with the text 'Online / Offline Activation'.

6. Click on the **Online** option.

7. Upon clicking on the **Online** option, enter the **Username** and **Password** and click on the **OK** button.
8. Upon clicking the **OK** button, the license gets activated.
 - a. If the license is issued as **Demo** then we see the Expiration Date, as shown below.

The screenshot shows the Milestone XProtect Management Client 2016 R3 interface. The main content area displays the following information:

Licensed
 Milestone C
 Vega Systems Inc.
 897 Fieldwood
 Thejaswi Bharadwaj
 Madepushi
 Your current level: Milestone Car
[Edit details...](#) [Access Milestone Care portal...](#)
[End-user license agreement](#) [Information about Milestone Care...](#)

Installed Prod

Product Version	Software License C	Expiration Date	Milestone Care Plus	Milestone Care Pre
XProtect Corporate 2016 R3 Pilot	M01-C01-102-05-6C	10/13/2017	N/A	N/A
SureStream v3.0.2	N/A	6/30/2017	6/30/2017	

License Overview - AI [License Details - All Sites...](#)

License Type	Activated
Hardware Device	3 out of 2000
ActiveActive	1 out of 1

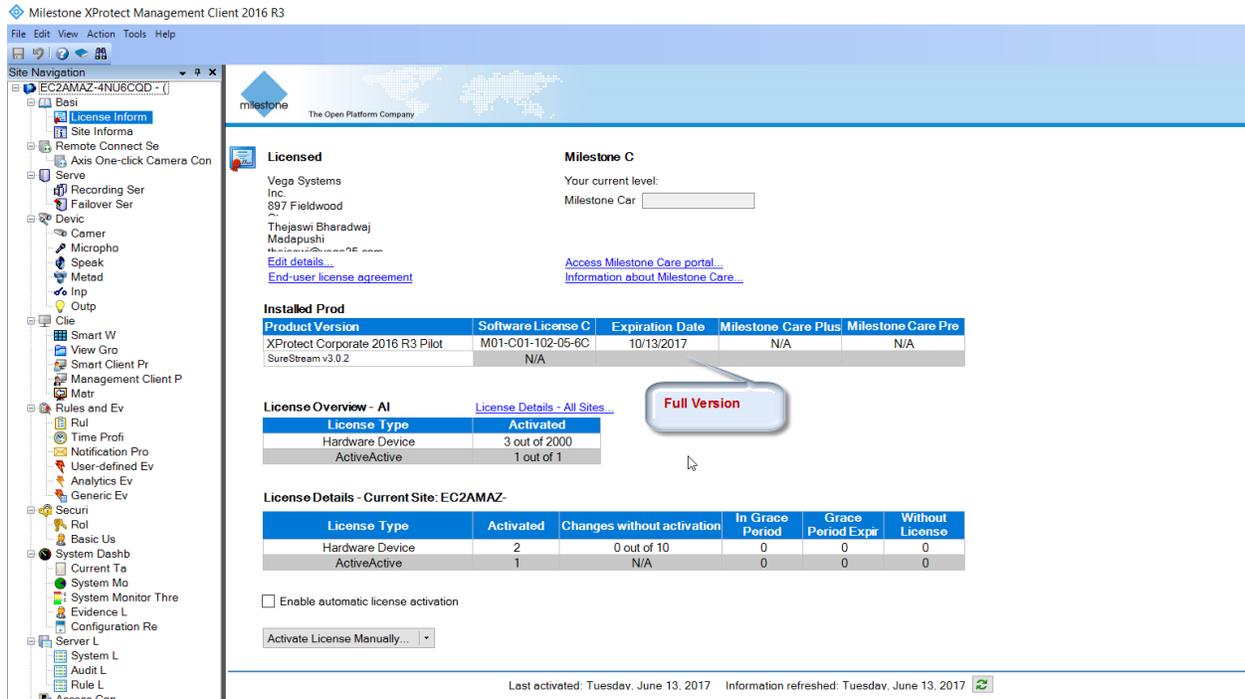
License Details - Current Site: EC2AMAZ-

License Type	Activated	Changes without activation	In Grace Period	Grace Period Expir	Without License
Hardware Device	2	0 out of 10	0	0	0
ActiveActive	1	N/A	1	0	0

Enable automatic license activation
 Activate License Manually...

Last activated: Tuesdav, June 13, 2017 Information refreshed: Tuesdav, June 13, 2017

- b. If the license is issued as **Full Version**, then we don't see any date in the Expiration Date column, as shown below.



Upgrading Software

To upgrade software,

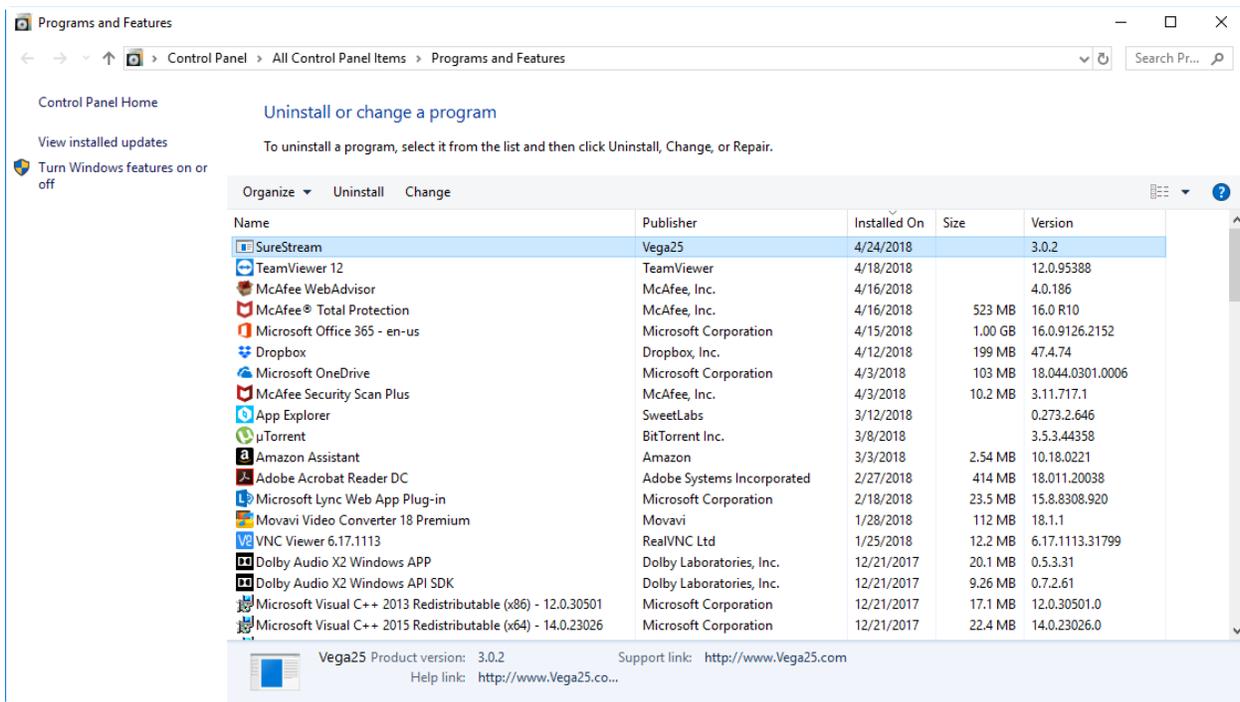
1. First, uninstall any versions by following un-installation instructions.
2. Then follow the installation instructions to install the latest version.
3. Finally, activate the license by following the License Activation instructions if the earlier license had expired.

Un-Installation

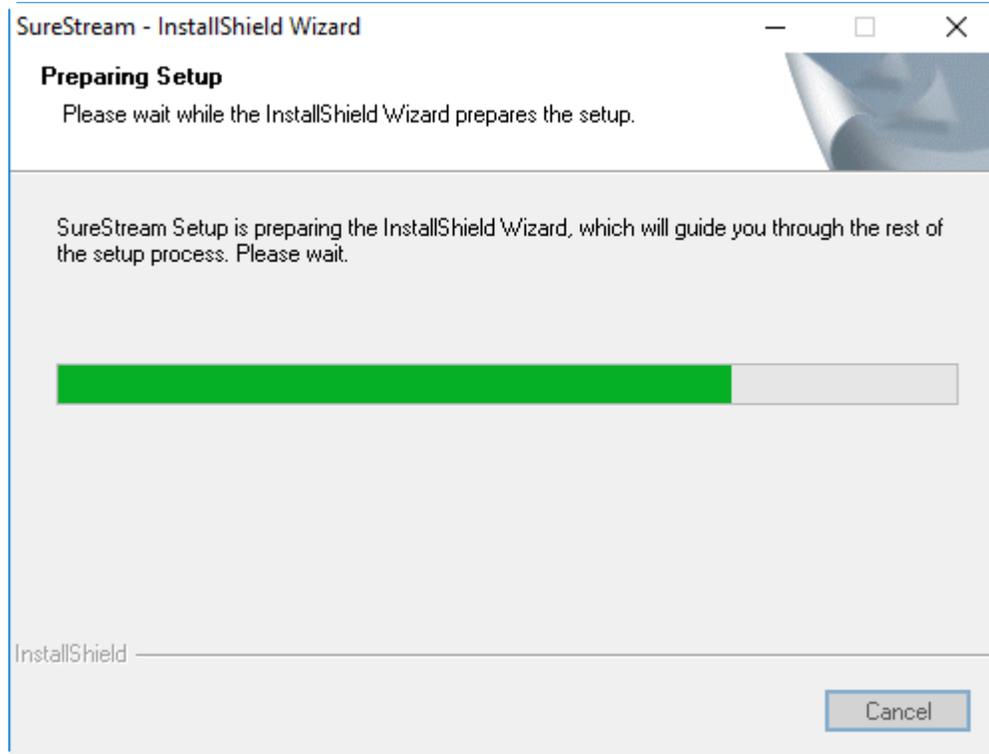
The steps below need to be repeated on the Management Server and each smart client system that is using the RMF plugin to uninstall the software.

1. If your Milestone software is active on the Management Server and Smart Client, please follow the shutdown procedure provided by Milestone, to stop all Milestone programs running on both Milestone Management Server and Smart Client. Then, follow the steps below:
2. Open the **Control Panel**.
3. Select **“SureStream”** from the list.

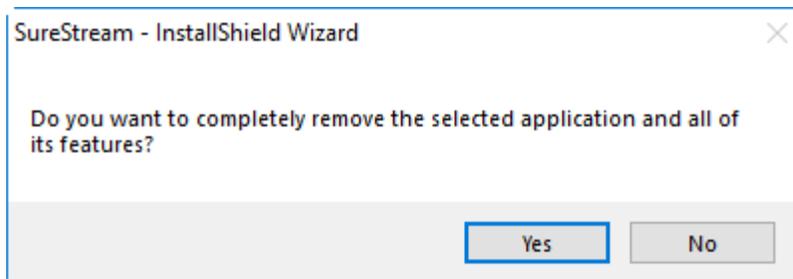
4. Click on the **“Uninstall”** button.



5. Upon clicking the uninstall button, the **“Preparing to Uninstall”** window will appear as shown in the below image.

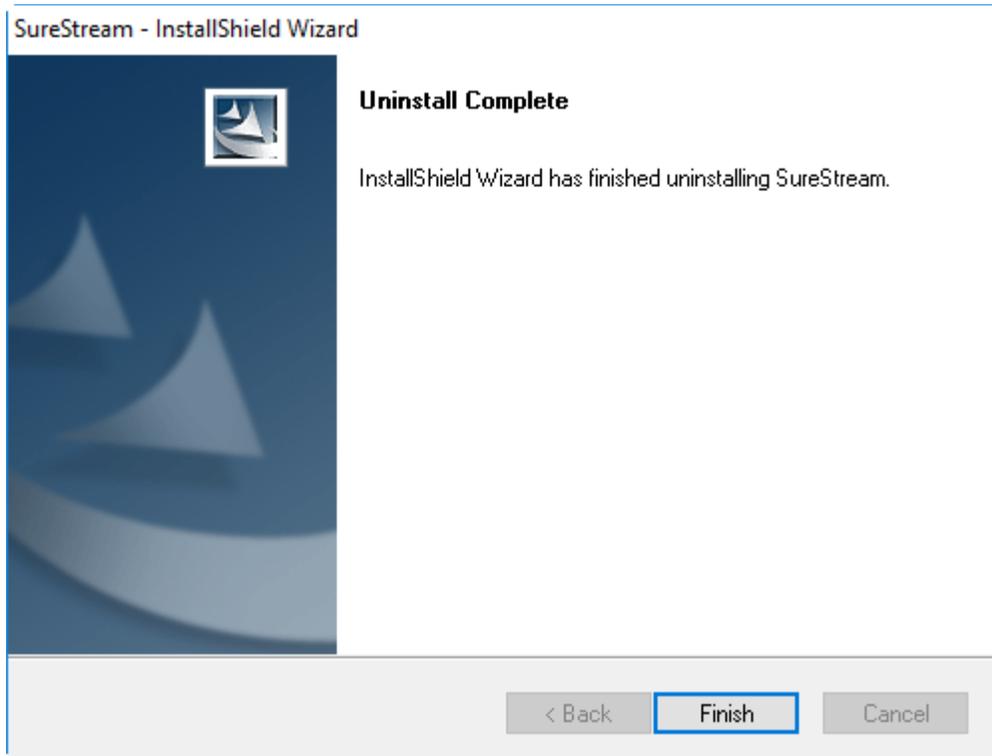


6. Once preparation is complete, the window below will appear.



7. Click on the **“Yes”** button.
8. Upon clicking on the **“Yes”** button, setup will get uninstalled.

9. Upon successful uninstallation, the below window will appear.



10. Click on the **“Finish”** button to complete the uninstallation.

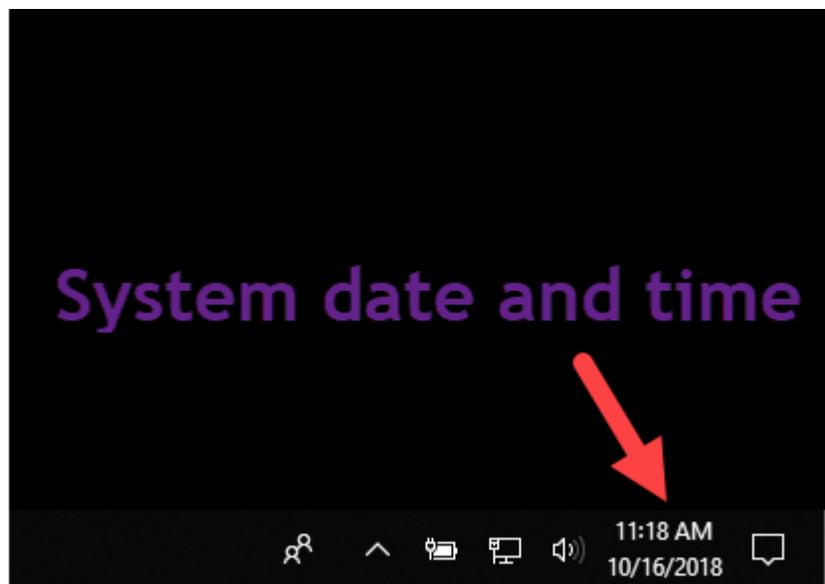
Things to check before running software

Step 1: Date and Time Sync in Camera and Smart Client Machines

Check to make sure that the Date and Time of cameras and Smart Client system are in sync.

If there are multiple smart client machines then all smart client machines date and time should be the same.

- a. Check the Date and Time of Smart Client System.



- b. Enter the IP address of the camera in the browser (Axis camera has taken for example)
- c. Click on Setup
- d. Click on Date & Time.

AXIS M5013 Network Camera Live View | Setup | Help

Basic Setup

Instructions

- 1 Users
- 2 TCP/IP
- 3 Date & Time
- 4 Video Stream
- 5 Audio Settings

Video & Audio

Live View Config

Detectors

Applications

Events

Recordings

Languages

System Options

About

Basic Setup

Before using the AXIS M5013 Network Camera, there are certain settings that should be made, most of which require Administrator access privileges. To quickly access these settings, use the numbered shortcuts to the left. All the settings are also available from the standard setup links in the menu.

Note that the only required setting is the IP address, which is set on the TCP/IP page. All other settings are optional. Please see the online help for more information.

Firmware version: 5.50.3.1
MAC address: AC:CC:8E:6E:93:DB

Date and Time Option

e. Click on “Synchronize with computer time ” option.

AXIS M5013 Network Camera Live View | Setup | Help

Date & Time Settings

Current Server Time

Date: 2018-10-16 Time: 11:14:01

New Server Time

Time zone: GMT-08 (Las Vegas, San Francisco, Vancouver)

Automatically adjust for daylight saving time changes.

Time mode:

Synchronize with computer time

Date: 2018-10-16 Time: 11:12:17

Synchronize with NTP server

NTP server: [No server specified](#)

Set manually

Date: 2018-10-16 Time: 11:13:55

Date & Time Format Used in Images

Specify date format: Predefined YYYY-MM-DD

Own %F

Specify time format: Predefined 24h With resolution: 1 second

Own %T

Save Reset

Synchronize with computer time

f. Click on “Save”.

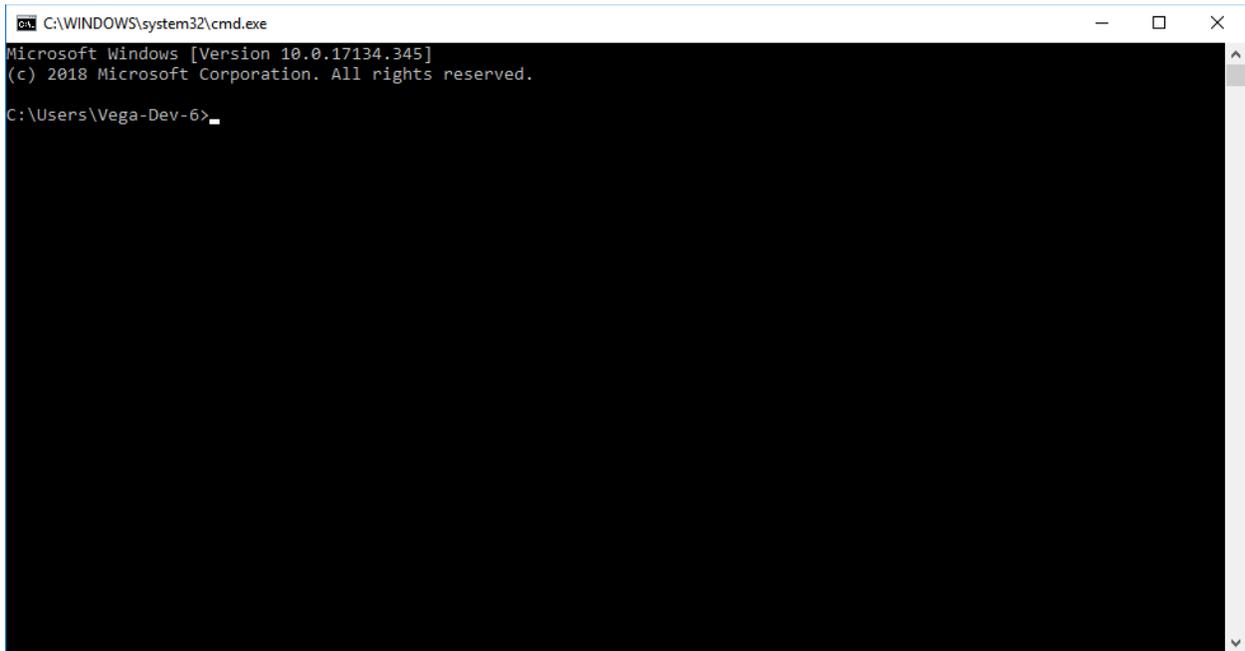
The screenshot shows the 'Date & Time Settings' page for an AXIS M5013 Network Camera. The page is divided into a left sidebar and a main content area. The sidebar contains a 'Basic Setup' menu with sub-items: 1 Users, 2 TCP/IP, 3 Date & Time (highlighted), 4 Video Stream, and 5 Audio Settings. Other sidebar items include Video & Audio, Live View Config, PTZ, Detectors, Applications, Events, Recordings, Languages, System Options, and About. The main content area has a title 'Date & Time Settings' and a help icon. It contains three main sections: 'Current Server Time' with date and time fields; 'New Server Time' with a time zone dropdown, an 'Automatically adjust for daylight saving time changes' checkbox, and three time mode options: 'Synchronize with computer time' (selected), 'Synchronize with NTP server' (with 'No server specified' as the NTP server), and 'Set manually'; and 'Date & Time Format Used in Images' with 'Specify date format' (Predefined: YYYY-MM-DD) and 'Specify time format' (Predefined: 24h, With resolution: 1 second). At the bottom of the settings are 'Save' and 'Reset' buttons. A red arrow points to the 'Save' button.

Save Button

Step 2: WiFi Disable in the Smart Client Machine.

Verify that the Smart Client machine has only one IP address and the machine is not connected through Wifi. Please follow the below steps to check.

- a. Open “*cmd prompt*”.

A screenshot of a Windows Command Prompt window. The title bar shows the path "C:\WINDOWS\system32\cmd.exe". The window content displays the following text: "Microsoft Windows [Version 10.0.17134.345]" followed by "(c) 2018 Microsoft Corporation. All rights reserved." and the current directory "C:\Users\Vega-Dev-6>". The prompt is followed by a cursor character. The rest of the window is black with no other text or commands visible.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Vega-Dev-6>
```

- b. Enter “*ipconfig*”.
- c. Wifi LAN adapter Wi-fi should be in a disconnected state.

```
C:\WINDOWS\system32\cmd.exe

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::5850:349c:586d:bd8a%11
    IPv4 Address. . . . . : 172.16.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.0.1

Ethernet adapter Bluetooth Network Connection 2:

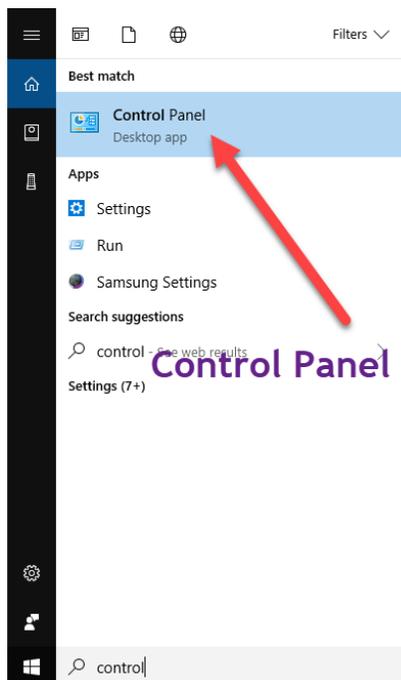
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\Vega-Dev-6>
```

Wi-fi adapter disconnected

One IP address

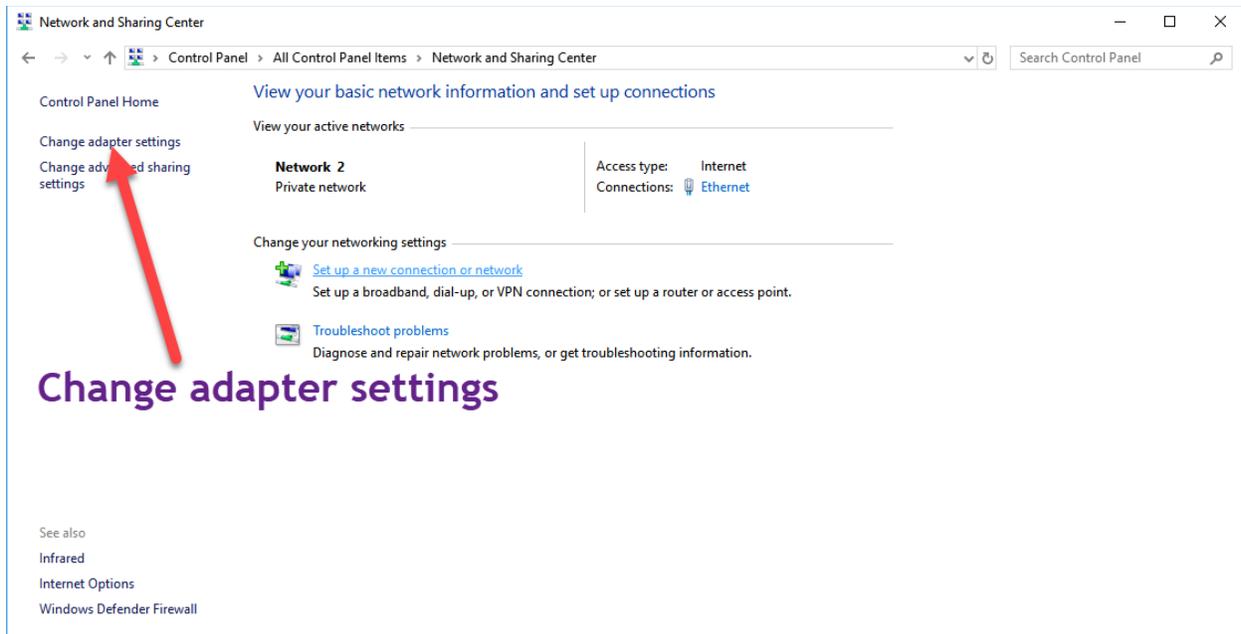
- d. If Wifi LAN adapter is not in disconnected state please disconnect Wifi as mentioned below.
 - i. Click on “Control” on windows search option and click on “Control Panel”.



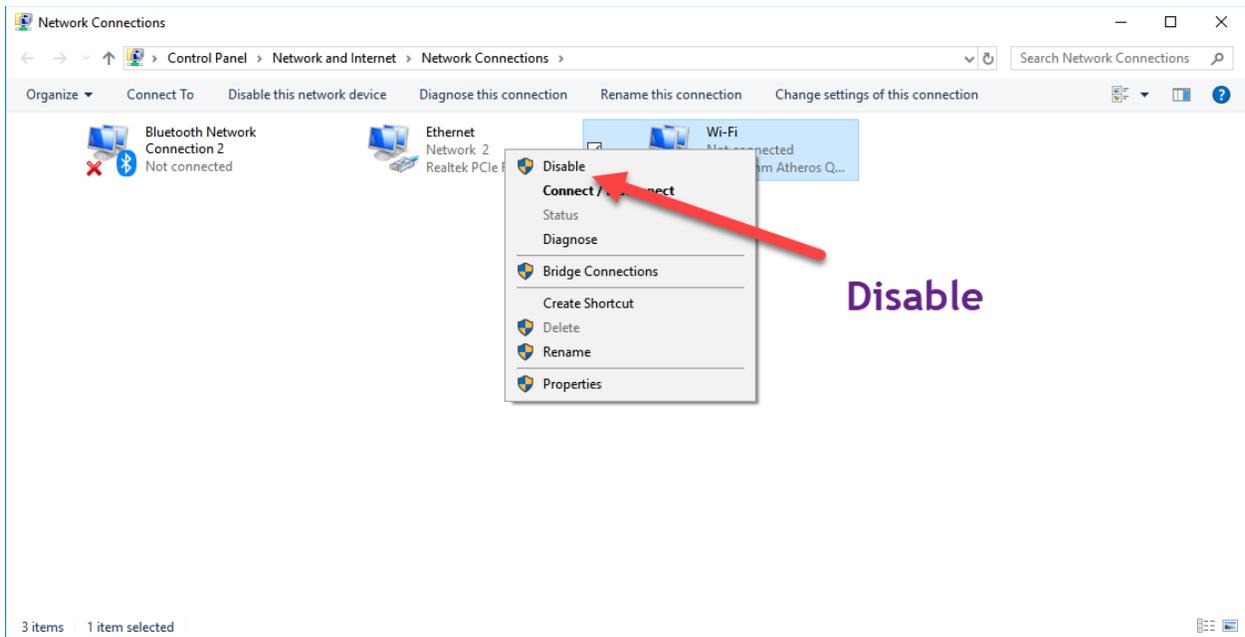
- ii. Click on “Network and Sharing Center”.



iii. Click on “Change adapter settings”.



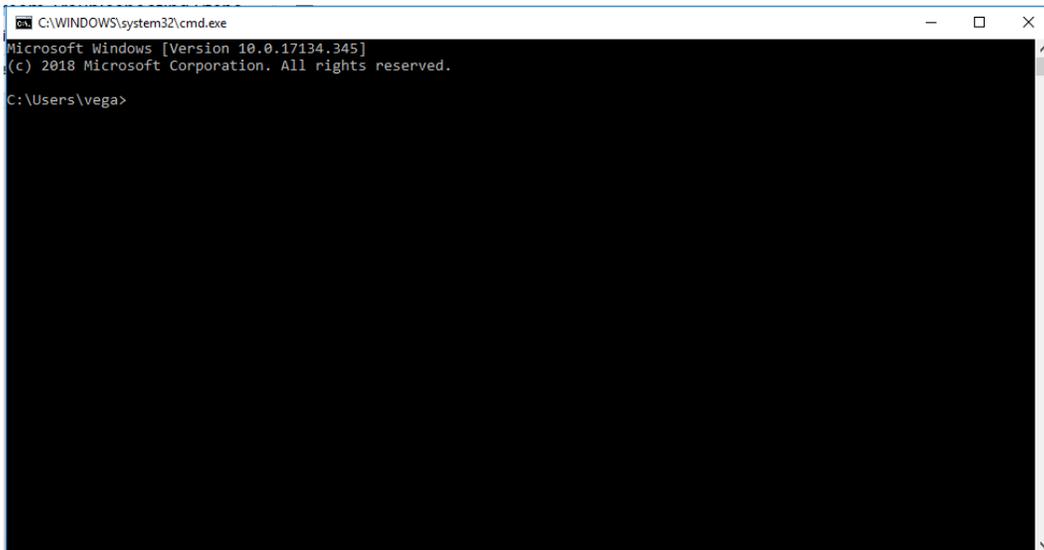
iv. Right click on the Wi-fi interface and click on “Disable”.



Step 3: Virtual Machine Adapter Disable in Smart Client Machine

Check if VMware / Hyper-V / VirtualBox etc. network adapters are disabled in the Smart Client machine. Please follow the below steps to check

- a. Open *"cmd prompt"*.

A screenshot of a Windows Command Prompt window. The title bar reads "C:\WINDOWS\system32\cmd.exe". The window content shows the following text: "Microsoft Windows [Version 10.0.17134.345]", "(c) 2018 Microsoft Corporation. All rights reserved.", and "C:\Users\vega>". The rest of the window is black, indicating that the rest of the command prompt output is not visible or has been obscured.

- b. Enter *"ipconfig"*.
- c. Only "Ethernet Lan" adapter should be enabled.

```

C:\WINDOWS\system32\cmd.exe

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::5850:349c:586d:bd8a%11
    IPv4 Address. . . . . : 172.16.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.0.1

Ethernet adapter Bluetooth Network Connection 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

C:\Users\Vega-Dev-6>

```

One IP address

- d. If there is any VMware / Hyper-V / VirtualBox etc. installed in Smart Client Machine then, all virtual machine ethernet adapters should be disabled as mentioned below

```

C:\WINDOWS\system32\cmd.exe

C:\Users\vega>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 13:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : Fe80::5b8:c816:f92a:c67c%20
    IPv4 Address. . . . . : 192.168.38.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : Fe80::485b:486c:a1d7:6822%3
    IPv4 Address. . . . . : 192.168.186.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter MI-F11:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : Fe80::58b5:af8a:0e07:f329%5
    IPv4 Address. . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::76da:daff:fe11:508e%5
    192.168.1.1

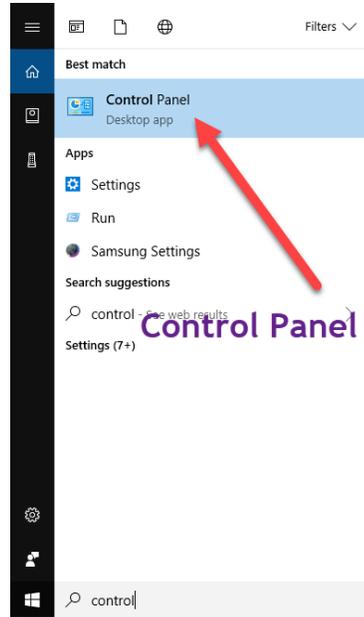
C:\Users\vega>

```

VMware adapters

LAN adapter

- i. Click on “Control” on windows search option and click on “Control Panel”.



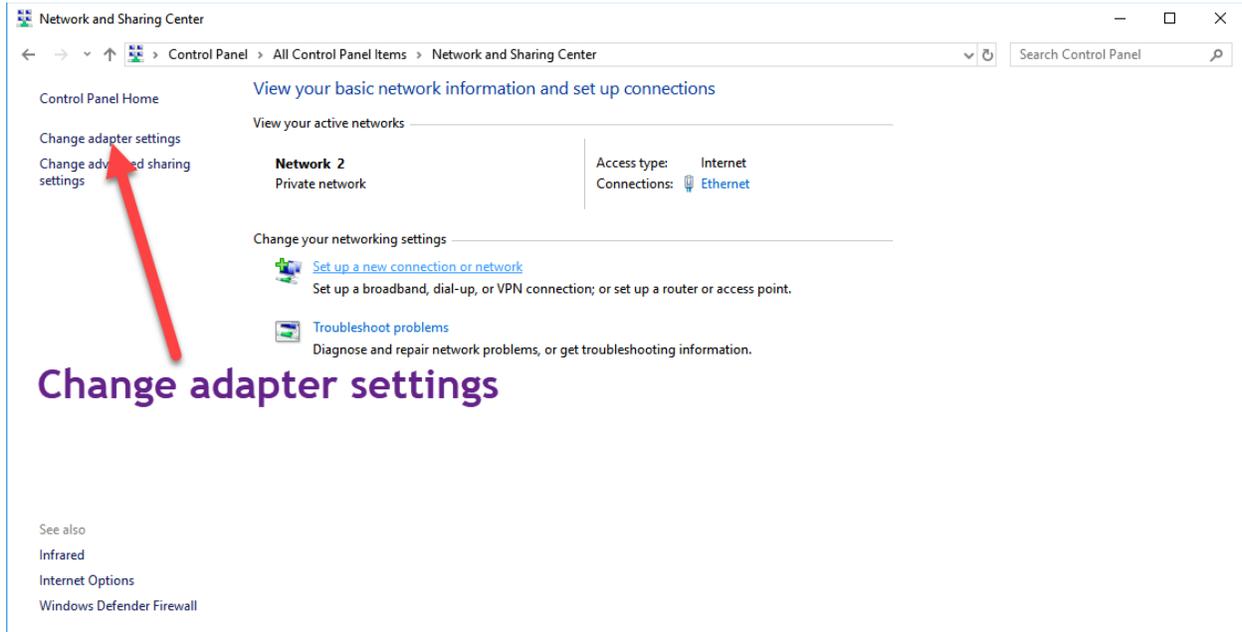
ii. Click on “Network and Sharing Center”.

Adjust your computer's settings

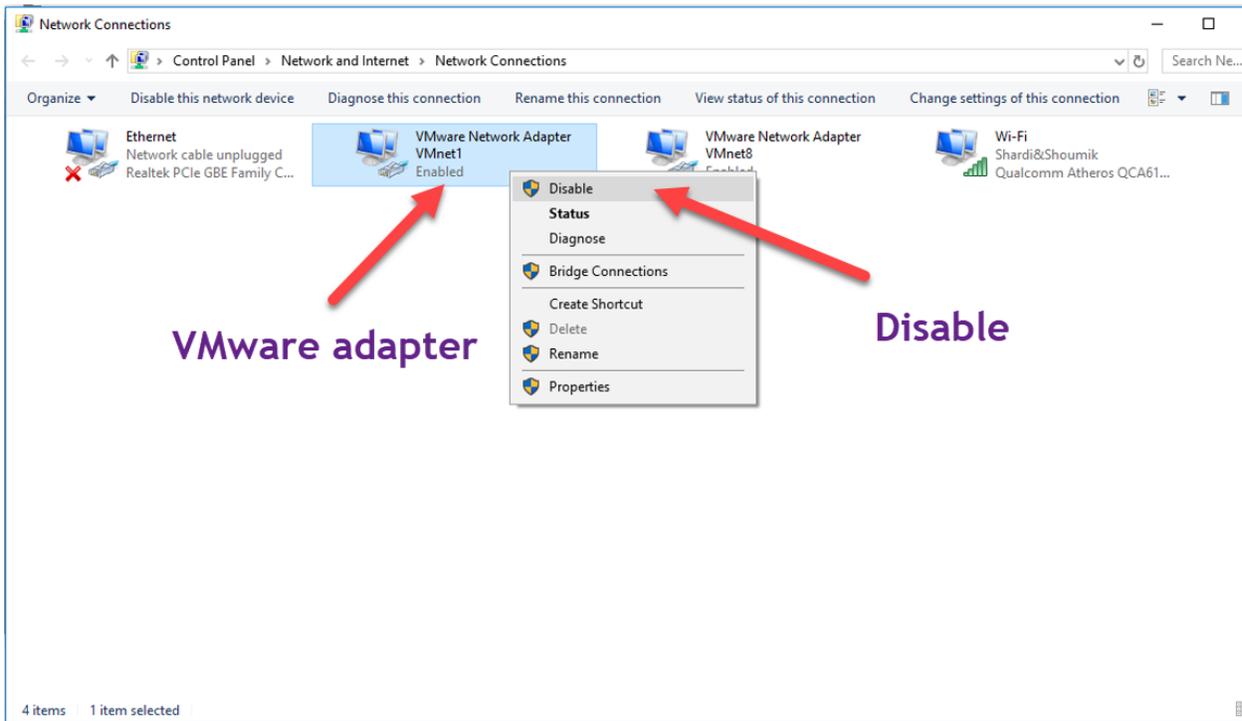
View by: Small icons ▾



iii. Click on “Change adapter settings”.



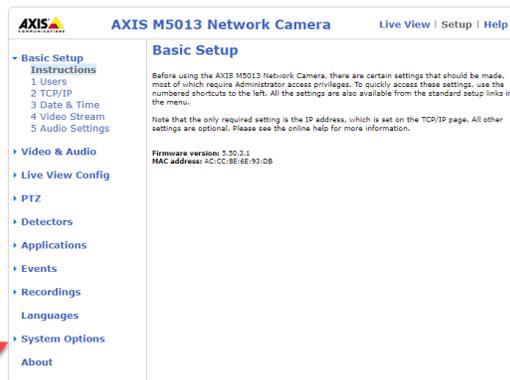
iv. Right click on all the VMware network adapters and click on “Disable”.



Step 4: Replay attack mode should be off in camera (specifically for Axis camera)

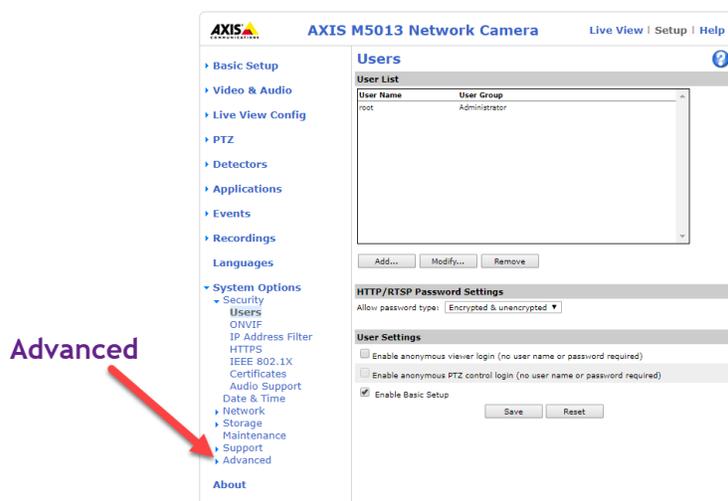
Follow the below procedures to disable “Replay attack mode” in camera (especially for Axis camera)

- Open the IP camera on the web browser.
- Click on “Setup”
- Click on “System Option”.



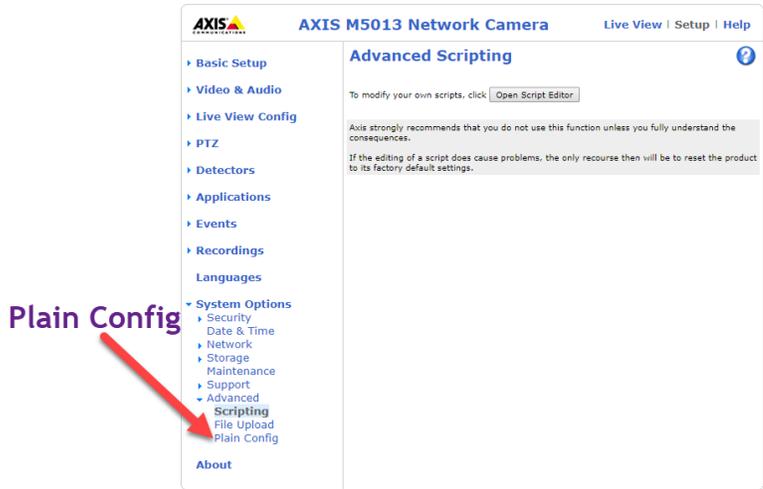
System Options

- Click on “Advanced” Option.



Advanced

- Click on “Plain Config”



f. The config below window appears.

The plain config page allows direct access to all the configurable parameters supported by the AXIS M5013 Network Camera. This page uses no extra scripts (Javascript or otherwise) and should function correctly in any browser or PDA. Select the parameter group to modify and configure the settings directly.

For help on parameters, please refer to the relevant help page available from the standard setup tools.

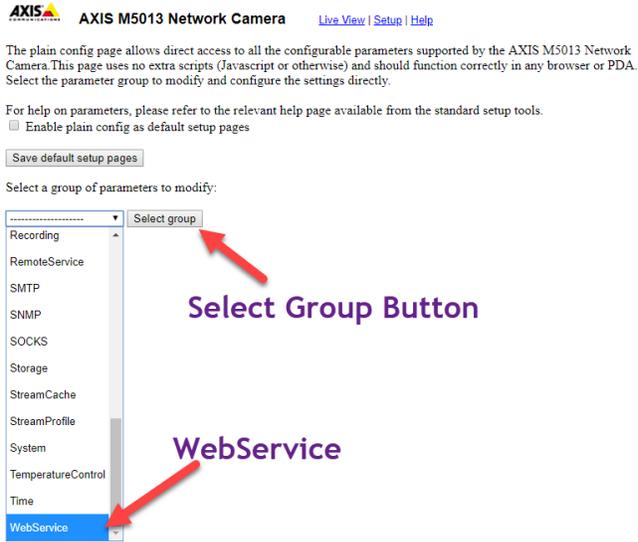
Enable plain config as default setup pages

[Save default setup pages](#)

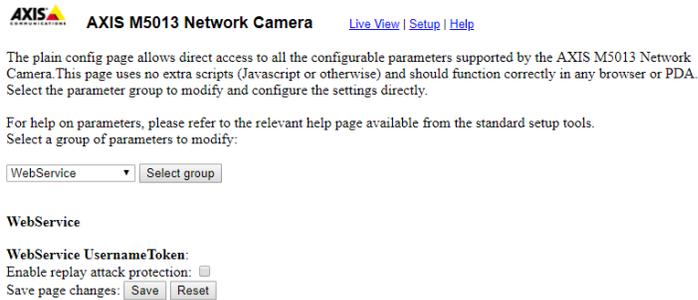
Select a group of parameters to modify:

..... ▾ [Select group](#)

g. Select “Web Service” in Select Group and click on Select Group button.



h. The below window will appear.



- i. Uncheck the “Enable replay attack protection” option and click on save button.

 **AXIS M5013 Network Camera** [Live View](#) | [Setup](#) | [Help](#)

The plain config page allows direct access to all the configurable parameters supported by the AXIS M5013 Network Camera. This page uses no extra scripts (Javascript or otherwise) and should function correctly in any browser or PDA. Select the parameter group to modify and configure the settings directly.

For help on parameters, please refer to the relevant help page available from the standard setup tools. Select a group of parameters to modify:

WebService

WebService

WebService UsernameToken:
Enable replay attack protection:
Save page changes:

Check Box

Save Button

Contact Us

Vega Systems Inc.,
1999 S Bascom Ave #700,
Campbell, CA 95008
USA
sales@vega25.com